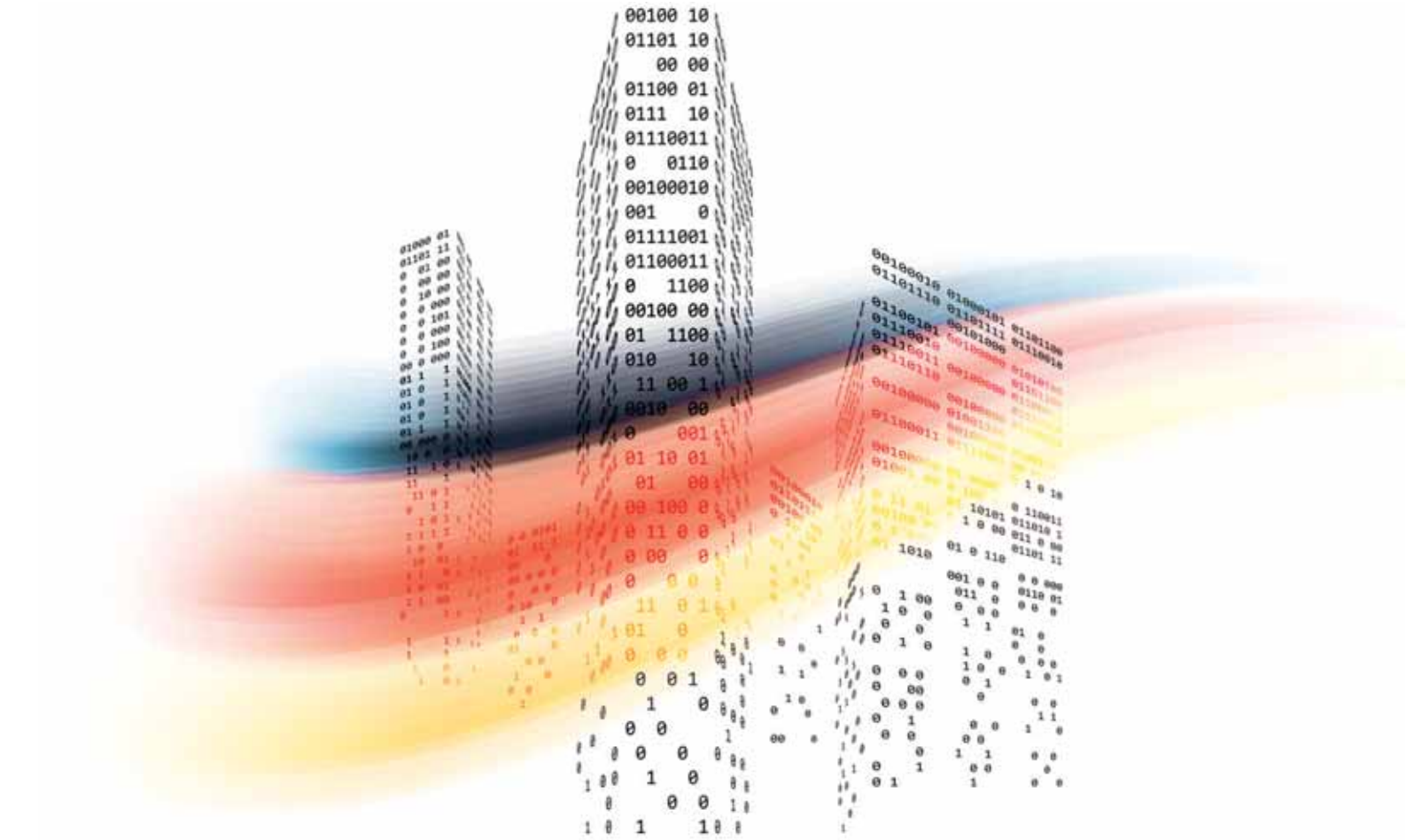
OKTOBER 2017

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT
Made in Germany



Datensicherheit

Endpoint Security **APT**

Ransomware Data Leakage

Compliance Verschlüsselung

Patch Management

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

Eine Publikation von IT-BUSINESS Security Insider

Trifft es **einen**, trifft es **alle**

itsa 2017
Die IT-Security Messe und Kongress
The IT Security Expo and Congress

Besuchen Sie uns:
Halle 9,
Stand 438

G DATA Unternehmenslösungen mit Anti-Ransomware-Technologie schützen die Endpoints in Ihrem Netzwerk **wirkungsvoll vor Cyber-Angriffen.**

- Einfache Installation und zentrale Verwaltung
- Modularer Aufbau, individuell anpassbar
- Verfügbar als Managed Service On-Premise oder in der Cloud

Jetzt Endpoints absichern – vom Smartphone bis zum Mail-Server
Mehr Infos auf **www.gdata.de/business**

G DATA
TRUST IN GERMAN SICHERHEIT

IT-Sicherheit ohne Hintertüren!

Dr. Holger Mühlbauer
Geschäftsführer
TeleTrusT –
Bundesverband
IT-Sicherheit e.V.

Liebe Leserinnen und Leser,

Wirtschaft und Verwaltung sowie private Anwender sind mehr denn je auf sichere und vertrauenswürdige Informationsinfrastrukturen angewiesen. Deutsche und europäische Gesetzgeber haben in den vergangenen Jahren begonnen, hierfür die Rahmenbedingungen zu schaffen. Leider gibt es mit dem Bundestrojaner auch Entwicklungen, die einer Erhöhung der IT-Sicherheit entgegenwirken können. Für das Ausspähen von verdächtigen Personen durch Strafverfolgungsbehörden werden in Zukunft vermutlich auch Sicherheitslücken genutzt, die nicht oder erst spät an die Hersteller gemeldet und dadurch bewusst offengehalten werden. Damit würde die IT-Sicherheit aller gesenkt. Kriminelle, die ebenfalls im Besitz dieses Wissens sind, könnten diese Lücken länger als notwendig ausnutzen. Diese Entwicklung sehen wir kritisch.

Als Bundesverband IT-Sicherheit e.V. sind wir bestrebt, die Sicherheit in der IT zu erhöhen. Gemeinsam mit Politik, Wirtschaft und den einschlägigen Herstellern wollen wir die Digitalisierung mit einem hohen Sicherheitsniveau der eingesetzten Systeme vorantreiben. Staatliche Anreize und eine staatliche Vorbildrolle im IT-Sicherheitsbeschaffungswesen sollten Investitionen in Zukunftstechnologien unterstützen. Die Wirtschaft ist hier ebenso gefordert, notwendige Technologien und Prozesse einzuführen, Mitarbeiter zu schulen und dadurch die vorhandene Technik effektiv zum Einsatz zu bringen. Die IT-Sicherheitsindustrie bietet sich mit der TeleTrusT-Initiative „IT Security made in Germany“ dabei als Kooperationspartner an. Die beteiligten deutschen IT-Sicherheitsunternehmen stehen gemeinsam für mehr Vertrauenswürdigkeit und Informationssicherheit ein, in dem sie sich zu grundlegenden Regeln verpflichtet haben, wie u.a. keine Backdoors in ihre Produkte einzubauen.

Diese Sonderpublikation informiert Sie über Lösungen, die deutsche Unternehmen im Bereich der IT-Sicherheit entwickelt haben. Gemeinsam mit den TeleTrusT-Mitgliedern wünsche ich Ihnen eine informative Lektüre und hoffe, dass Sie zahlreiche Anregungen erhalten, um die IT-Sicherheit im Unternehmen, in Ihrer Behörde und auch in Ihrem privaten Umfeld weiter zu stärken. □

IT-SICHERHEIT AUS DEUTSCHLAND

IT-SICHERHEIT AUS DER CLOUD

VERSCHLÜSSELUNG

DATENSCHUTZ UND COMPLIANCE

INDUSTRIE 4.0 UND INTERNET DER DINGE

REDAKTION

Titelbild: © leszekglasner/Artenauta - stock.adobe.com (M) Carin Boehm

TeleTrusT-Initiative „IT Security made in Germany“

„ITSMIG“ („IT Security made in Germany“) wurde 2005 auf Initiative des Bundesministeriums des Innern (BMI), des Bundesministeriums für Wirtschaft und Technologie (BMWi) sowie Vertretern der deutschen IT-Sicherheitswirtschaft etabliert und 2008 in einen eingetragenen Verein überführt. Sowohl BMI als auch BMWi hatten eine Schirmherrschaft übernommen.
Nach intensiven Erörterungen sind TeleTrusT und ITSMIG 2011 übereingekommen, dass sich auf ihren Handlungsfeldern Synergien erschließen lassen. Zukünftig werden die ITSMIG-Aktivitäten unter dem Dach des TeleTrusT als eigenständige Arbeitsgruppe „ITSMIG“ fortgeführt.

Die TeleTrusT-Arbeitsgruppe „ITSMIG“ verfolgt das Ziel der gemeinsamen Außendarstellung der an der Arbeitsgruppe mitwirkenden Unternehmen und Institutionen gegenüber Politik, Wirtschaft, Wissenschaft und Öffentlichkeit auf deutscher, europäischer bzw. globaler Ebene. BMWi und BMI sind im Beirat der Arbeitsgruppe vertreten.

Stabilität kommt von Architektur: Netzwerksicherheit mit SINA.

Wer täglich mit vertraulichen Daten arbeiten muss, braucht eine ganzheitliche Lösung für eine sichere Netzwerk-Architektur: SINA von secunet. Anders als bei einem Flickwerk aus schlecht harmonisierenden Einzelkomponenten administrieren Sie mit SINA alle Bausteine über ein zentrales Management. Mit SINA werden Sicherheit und Komfort zu einer Einheit. Dazu besitzt SINA mit die höchsten Zulassungen durch BSI, EU und NATO und ist ohne Grenzen skalierbar für Arbeitsumgebungen bis hin zu mehreren Tausend Arbeitsplätzen.

IT security „Made in Germany“.
www.secunet.com/sina

secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland

Vertrauen hat einen Namen

Mit der Vergabe des Vertrauenszeichens „IT Security made in Germany" an deutsche Anbieter erleichtert der TeleTrusT – Bundesverband IT-Sicherheit e.V. Endanwendern und Unternehmen die Suche nach vertrauenswürdigen IT-Sicherheitslösungen.

Von Dr. Holger Mühlbauer und Jürgen Paukner

Träger des Vertrauenszeichens „IT Security made in Germany" (Stand 21.9.2017)

- 1984not Security GmbH
- 8ack GmbH
- abl social federation GmbH
- Accellence Technologies GmbH
- achelos GmbH
- Achtwerk GmbH & Co. KG
- ads-tec GmbH
- akquinet enterprise solutions gmbH
- ALLGEIER IT SOLUTIONS GmbH
- ANMATHO AG
- Antago GmbH
- apsec Applied Security GmbH
- ASOFTNET
- ATIS systems GmbH
- Avira GmbH & Co. KG
- Backes SRT GmbH
- BCC Unternehmensberatung GmbH
- bc digital GmbH
- Bechtle GmbH & Co. KG
- befine Solutions AG
- Beta Systems IAM Software AG
- Biteno GmbH
- Blue Frost Security GmbH
- bowbridge Software GmbH
- Brainloop AG
- Bundesdruckerei GmbH
- CBT Training & Consulting GmbH
- CCVOSSEL GmbH
- cdt consulting // Carolin Desirée Töpfer
- certgate GmbH
- CHIFFRY GmbH
- Clinc GmbH
- Cloud Identity and Access Management (C-IAM)
- cloudTEC GmbH
- CoCoNet Computer-Communication Networks GmbH
- Cognitec Systems GmbH
- COMback Holding GmbH
- commocial GmbH
- consistec Engineering & Consulting GmbH
- Consultix GmbH
- CONTURN Analytical Intelligence Group GmbH
- Crashtest Security GmbH
- CryptoMagic GmbH
- CryptoTec AG
- CSO GmbH
- cv cryptovision GmbH
- CycleSEC GmbH
- CYPP GmbH
- dacoso data communication solutions GmbH
- dal33t GmbH
- Daniel Aßmann – Datenschutz & QM
- DATAKOM GmbH
- DATUS AG
- DERMALOG Identification Systems GmbH
- Detack GmbH
- DeviceLock Europe GmbH
- DFN-CERT Services GmbH
- digitalDefense Information Systems GmbH
- digitronic computersysteme GmbH
- DIGITTRADE GmbH
- DocRAID – professional data privacy protection
- DriveLock SE
- e-ito Technology Services GmbH
- ecsec GmbH
- Elaborated Networks GmbH
- eperi GmbH
- esatus AG
- essendi it GmbH
- exceet Secure Solutions AG
- Fiducia & GAD IT AG
- FSP GmbH
- FZI Forschungszentrum Informatik
- G Data Software AG
- genua GmbH
- Giegerich & Partner GmbH
- Glück & Kanja Consulting AG
- Governikus GmbH & Co. KG
- GROUP Business Software Europa GmbH
- grouptime GmbH

Die Verwendung des markenrechtlich geschützten TeleTrusT-Vertrauenszeichens „IT Security made in Germany“ wird interessierten Anbietern durch TeleTrusT auf Antrag und bei Erfüllung der nachstehenden Kriterien zeitlich befristet gestattet:

1. Der Unternehmenshauptsitz muss in Deutschland sein.
2. Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten.
3. Die angebotenen Produkte dürfen keine versteckten Zugänge enthalten (keine „Backdoors“).
4. Die IT-Sicherheitsforschung und -entwicklung des Unternehmens muss in Deutschland stattfinden.
5. Das Unternehmen muss sich verpflichten, den Anforderungen des deutschen Datenschutzrechtes zu genügen.

Die Liste der zertifizierten deutschen Unternehmen wächst beständig und ist deshalb tagesaktuellen Änderungen unterworfen. Die aktuelle Liste der Unternehmen, denen die Nutzung des Vertrauenszeichens derzeit eingeräumt wird, können Sie einsehen unter: www.teletrust.de/itsmig/zeichentraeger/ □

- GZIS GmbH
- HiScout GmbH
- HOB GmbH & Co. KG
- Hornetsecurity GmbH
- ifAsec GmbH
- if(is) – Institut für Internet-Sicherheit
- Infineon Technologies AG
- Inlab Networks GmbH
- innovaphone AG
- isits AG International School of IT Security
- ITConcepts Professional GmbH
- IT-Sitter GmbH Deutschland
- ISL Internet Sicherheits-lösungen GmbH
- itWatch GmbH
- keepbit SOLUTION GmbH
- KeyIdentity GmbH
- KikuSema GmbH
- KIWI.KI GmbH
- KORAMIS GmbH
- LANCOM Systems GmbH
- limes datentechnik gmbh
- Link11 GmbH
- Linogate GmbH
- MaskTech GmbH
- MATESO GmbH
- MB Connect Line GmbH Fernwartungssysteme
- media transfer AG
- metafinanz Informations-systeme GmbH
- M&H IT-Security GmbH
- msts GmbH
- NATEK Technologies GmbH
- NETZWERK Software GmbH
- NCP engineering GmbH
- Net at Work GmbH
- netfiles GmbH
- NEOX NETWORKS GmbH
- Nexis GmbH
- nicos AG
- Nimbus Technologieberatung GmbH
- OctoGate IT Security Systems GmbH
- OTARIS Interactive Services GmbH
- PHOENIX CONTACT Cyber Security AG
- Pix Software GmbH
- PPI Cyber GmbH
- PRESENSE Technologies GmbH
- procilon IT-Solutions GmbH
- PROSTEP AG
- PSW GROUP GmbH & Co. KG
- Pyramid Computer GmbH
- QiTEC GmbH
- QGroup GmbH
- ReddFort Software GmbH
- RED Medical Systems GmbH
- retarus GmbH
- Rhebo GmbH
- Rohde & Schwarz Cybersecurity GmbH
- SAMA PARTNERS Business Solutions GmbH
- sayTEC AG
- SC-Networks GmbH
- Secomba GmbH
- secrypt GmbH
- secucloud GmbH
- SECUDOS GmbH
- secunet Security Networks AG
- Securepoint GmbH
- Sengi GmbH
- SerNet GmbH
- Steganos Software GmbH
- syracom consulting AG
- sys4 AG
- TDT GmbH
- TESIS SYSware Software Entwicklung GmbH
- True ITK – John Ollhorn
- TÜV Informationstechnik GmbH
- Ungeheuer IT UG
- Unify
- Uniscon GmbH
- Utimaco IS GmbH
- VegaSystems GmbH & Co. KG
- virtual solution AG
- WhosApp GmbH
- WMC Wüpper Management Consulting GmbH
- Xura Secure Communications GmbH
- ZenGuard GmbH
- Zertificon Solutions GmbH

G DATA Business Solutions 14.1: Effektiver Netzwerkschutz der nächsten Generation „Made in Germany“

Die deutsche Wirtschaft steht im Fadenkreuz von Cyberkriminellen. Laut Bitkom entsteht den Unternehmen jedes Jahr ein Schaden von rund 55 Milliarden Euro. Dabei bereiten insbesondere Erpressertrojaner, Datendiebstahl und Online-Attacken auf die Netzwerkstruktur IT-Verantwortlichen großes Kopfzerbrechen.
Auf der it-sa in Halle 9, Stand 438, stellt G DATA die neuen Businesslösungen 14.1 mit „Next Generation AV“ vor. Die neu integrierte Anti-Ransomware-Technologie lässt Erpressertrojanern keine Chance und verhindert so Datenverluste und Ausfälle der IT-Infrastruktur.

G DATA TRUST IN GERMAN SICHERHEIT

Spionage, Sabotage oder Datendiebstahl – die Folgen eines erfolgreichen Cyberangriffs sind für Unternehmen oft verheerend, denn Sie haben viel zu verlieren. Kundendatenbanken, Konstruktionspläne oder Zahlungsinformationen sind begehrte Diebesgüter. Der Verlust dieser Daten kann Firmen schnell in wirtschaftliche Bedrängnis bringen. Ein umfassender und effektiver Schutz der IT-Infrastruktur ist daher entscheidend. Die neuen G DATA Businesslösungen 14.1 – Antivirus Business, Client Security Business, Endpoint Protection Business und Managed Endpoint Security – vereinen die modernsten Security-Technologien der nächsten Generation in einem mehrschichtigen „Layered Security“-Konzept zu einem effektiven Schutzwall.

Proaktiver Schutz vor Ransomware

WannaCry, Locky oder Petya – Erpressertrojaner stehen bei Cyberkriminellen aktuell hoch im Kurs. Die Täter attackieren damit gezielt Unternehmen, um Datensätze oder ganze Systeme zu sperren und Geldbeträge zu erpressen. Mit dem neu integrierten Anti-Ransomware-Modul haben die Kriminellen keine Chance mehr und Unterneh-

mensnetzwerke sind gut geschützt. Die proaktive Technologie erkennt selbst bisher unbekannte Erpressertrojaner frühzeitig und wehrt sie zuverlässig ab.

Zentrale Netzwerkverwaltung

Dank des G DATA Administrators haben IT-Verantwortliche alle Windows-PCs, Macs und Linux-Rechner sowie deren jeweiligen Sicherheitsstatus immer im Blick. Durch die zentrale Konfiguration und Administration verringert sich der Arbeitsaufwand. Das integrierte Mobile Device Management sorgt dafür, dass auch alle iOS- und Android-Smartphones und -Tablets abgesichert sind. Die optionalen Module Patch Management und Network Monitoring runden den Unternehmensschutz ab.

G DATA bietet mit dem Layered-Security-Ansatz ein umfassendes und perfekt verzahntes Sicherheitskonzept für Unternehmensnetzwerke jeder Größe.

G DATA Garantie: die Kundendaten bleiben in Deutschland

Als deutscher IT-Security-Hersteller tritt G DATA für höchste Sicherheitsstandards ein und garantiert seinen Kunden und Partnern, dass alle Daten ausschließlich in Deutschland verbleiben und vor dem Zugriff Dritter geschützt sind. Darüber hinaus enthalten die G DATA Sicherheitslösungen keine Hintertüren für Geheimdienste oder andere Behörden.

Security as a Service

Unternehmen, die nicht über eine eigene EDV-Abteilung verfügen, brauchen dank G DATA Managed Endpoint Security keine Kompromisse hinsichtlich ihrer IT-Sicherheit einzugehen: Die Sicherheitslösung wird als „Security as a Service“ von einem vertrauenswürdigen IT-Dienstleister betrieben, der die Absicherung der IT-Systeme sicherstellt. Unternehmen können sich so voll und ganz auf ihr Tagesgeschäft konzentrieren. Mit Managed Endpoint Security powered by Microsoft Azure bietet G DATA eine auf die Azure-Plattform zugeschnittene Lösung. Der G DATA Partner betreibt dabei für seinen Kunden einen virtuellen Management Server in der Microsoft Cloud Deutschland – eine Plattform, die durch die Einhaltung der strengen deutschen Datenschutzgesetze den Compliance-Anforderungen für Public-Cloud-Lösungen gerecht wird. Kunden profitieren hierbei von einer hohen Verfügbarkeit und schnellen Skalierbarkeit.

Kathrin Beckert-Plewka, G DATA ■

Ein kostenfreies Whitepaper zu Layered Security können Sie auf www.gdata.de/whitepapers als PDF herunterladen. Weitere Informationen zu den G DATA Business-Lösungen finden Sie unter: www.gdata.de/business

G DATA auf der it-sa: Halle 9, Stand 438

Deutsche IT-Sicherheit auf dem Vormarsch

In Zeiten immer komplexerer Netzwerke gewinnt das Thema Datensicherheit zunehmend an Bedeutung. Weltweit befindet sich der Markt für IT-Sicherheitslösungen im Wachstum. Deutsche Cyber Security-Unternehmen sind auf dem besten Wege, hier eine zentrale Rolle zu spielen. Ist „Made in Germany" doch mittlerweile auch im IT-Sicherheitsgewerbe ein Synonym für hohe qualitative Standards geworden.

Von Udo Kalinna, IFASEC

Entscheidend vorangetrieben haben diese Entwicklung die politischen Weichenstellungen von Bundesregierung und Bundestag der letzten Jahre. Innovative Sicherheitslösungen sind entstanden, die weltweit ihresgleichen suchen.

Deutschland – Nährboden für IT-Sicherheit der nächsten Generation

Bereits vor Jahren hat die Bundesregierung Maßnahmen ergriffen, um das Innovationspotential deutscher IT-Sicherheitsdienstleister zu erhöhen und die deutsche Online-Infrastruktur mit Sicherheitsprodukten made in Germany auszustatten. Der Erfolg kann sich mittlerweile sehen lassen. So kam „Microsoft's Security Intelligence Report" 2016 zu dem Ergebnis, dass Rechner und Netzwerke in Deutschland im internationalen Vergleich deutlich seltener von Malware-Angriffen betroffen sind. Allein im 2. Quartal 2016 lag ihre Quote rund 40 Prozent unterhalb des internationalen Durchschnitts. Ursache dieses Erfolges ist nicht zuletzt die enge Zusammenarbeit zwischen Privatwirtschaft und Politik.

Letztere hat erkannt, dass das Gebiet der IT-Sicherheit ein erhebliches Wachstumspotential und sicherheitstechnische Breitenwirkung für die gesamte deutsche Wirtschaft in sich birgt. Auch deshalb wurde am 9. November 2016 von der Bundesregierung die „Cyber-Sicherheitsstrategie für Deutschland" beschlossen. Mit dieser nimmt die Bundesrepublik Deutschland international eine Vorreiterrolle ein. Im letzten Jahr hat die Bundesrepublik mit ihrem Vorsitz in der Organisation für Sicherheit und Zusammenarbeit in Europa diesen Anspruch bereits unter Beweis stellen können. Zahlreiche vertrauensstiftende Maßnahmen konnten unter dem deutschen Vorsitz im Bereich der Cybersicherheit erfolgreich umgesetzt werden.

Basis der neuen Cyber-Sicherheitsstrategie ist das seit Juli 2015 rechtskräftige bundesdeutsche „IT-Sicherheitsgesetz". In ihm werden Privatunternehmen in die Pflicht genommen, erkannte Angriffe auf ihre Daten kenntlich zu machen und sich mit dem Bundesamt für Sicherheit in der Informationstechnik auszutauschen. Mangelnder Datenaustausch war und ist weltweit die zentrale Schwachstelle moderner IT-Sicherheit. Nur wenige Unternehmen geben einen erfolgreichen Angriff auf ihre Netzwerke offen zu. IT-Sicherheitsexperten und Kunden

können sich deshalb meist nur ein unvollständiges Bild von der Datensicherheit eines Unternehmens und der allgemeinen Gefahrenlage im Internet machen. Dabei sind doch gerade diese Daten ein zentraler Baustein, will man effiziente Lösungen zur Abwehr von Hackerangriffen entwickeln. So hilft das IT-Sicherheitsgesetz nicht nur dabei, deutsche Sicherheitspolitiken und -praktiken zu verbessern, sondern wertet auch den deutschen Standort für IT-Sicherheitsunternehmen weiter auf.

IT-Security aus Deutschland: Industrie 4.0 und geringer Administratoraufwand im Blick

Doch was sind die Herausforderungen, vor denen deutsche Hersteller von IT-Sicherheitssoftware bei der Entwicklung stehen? Um zukunftsfähig zu bleiben und höchste Sicherheit zu gewährleisten, müssen sie sowohl die steigende Komplexität innerhalb der Netzwerke als auch die personelle Unterbesetzung der Sicherheitsabteilungen bei der Entwicklung berücksichtigen.
Wie bereits erwähnt, bringt die mit der Digitalisierung einhergehende Effizienzsteigerung zweifellos auch gravierende Sicherheitsrisiken mit sich. Das Problem scheint hier auf der Hand zu liegen: Die höhere Komplexität innerhalb der Netzwerke geht unweigerlich mit einer Erhöhung der potenziellen Angriffspunkte einher. Ein weiterer Punkt ist die Tatsache, dass IT-Sicherheitsabteilungen häufig personell unterbesetzt sind. Heutzutage setzt sich immer mehr die Ansicht durch, die mehrheitlich heterogenen IT-Sicherheitsanwendungen müssen zentral verwaltet werden, ansonsten würden diese zu bloßen Sicherheitssilos verkommen. IT-Sicherheitsfachkräfte sind imstande, Rohdaten in einer derart zentralen Anwendung wie beispielsweise einem SIEM-Server zu lesen, zu interpretieren und schließlich angemessen zu reagieren. Doch gerade diese IT-Sicherheitskräfte sind in der heutigen Zeit schwer zu finden.

Software Defined Security

Eine Art von Sicherheitslösungen, die den Administratorenaufwand auf ein Minimum reduziert und gleichzeitig der hohen Komplexität innerhalb der Netzwerke gerecht wird, sind die sogenannten Software Defined Security (SDSec)-Lösungen. Wichtig ist hier eine einfache Integration in die komplexen Netzwerkstrukturen und eine übersichtliche Benutzeroberfläche samt homogenisierten Metadaten. Ähnlich dem Software Defined Networking, bei dem die Netzwerkkontrolle getrennt vom zu kontrollierenden Netzwerk erfolgt, erfolgt beim SDSec die Sicherheitskontrolle gelöst von den einzelnen Sicherheitsprozessen. SDSec eröffnet so die Möglichkeit, Netzwerksicherheit zu virtualisieren und sämtliche Überwachungsprozesse in einem logischen System zu managen.
Eine effektive SDSec-Lösung scannt automatisiert zunächst das Netzwerk, erfasst und katalogisiert sämtliche Endgeräte sowie die darauf laufenden Dienste. Der Administrator sollte in der Lage sein, einzelne Dienste, ganze Geräte oder einzelne Ports auch individuell zu steuern, zu konfigurieren oder komplett abzuschalten. Informationen anderer Sicherheitslösungen laufen hier auf einer Plattform – übersichtlich und leicht verständlich präsentiert – zusammen. □

Der Autor

Udo Kalinna hatte von 2010–2017 eine Verwaltungsprofessur für IT-Sicherheit an der Hochschule Emden/Leer inne und ist dort weiterhin als Dozent tätig. Er ist Firmengründer der IFASEC GmbH aus Dortmund. Nach dreijähriger Entwicklungsarbeit und rund einem Dutzend Feldversuchen hat IFASEC nun seine Software Defined Security (SDSec)-Plattform SCUDOS zur Marktreife geführt.

Cloudbasierte WAFs als Garant für die Einhaltung des neuen IT-Sicherheitsgesetzes

Dass IT-Sicherheit ein sehr wichtiges Thema ist, wissen wir nicht erst seit dem WannaCry-Vorfall. Dieser hat aber noch einmal deutlich gemacht, dass bei vielen Firmen IT-Sicherheit stark vernachlässigt wird.

Von Swjatoslav Cicer, Net Wächter (GZIS GmbH)

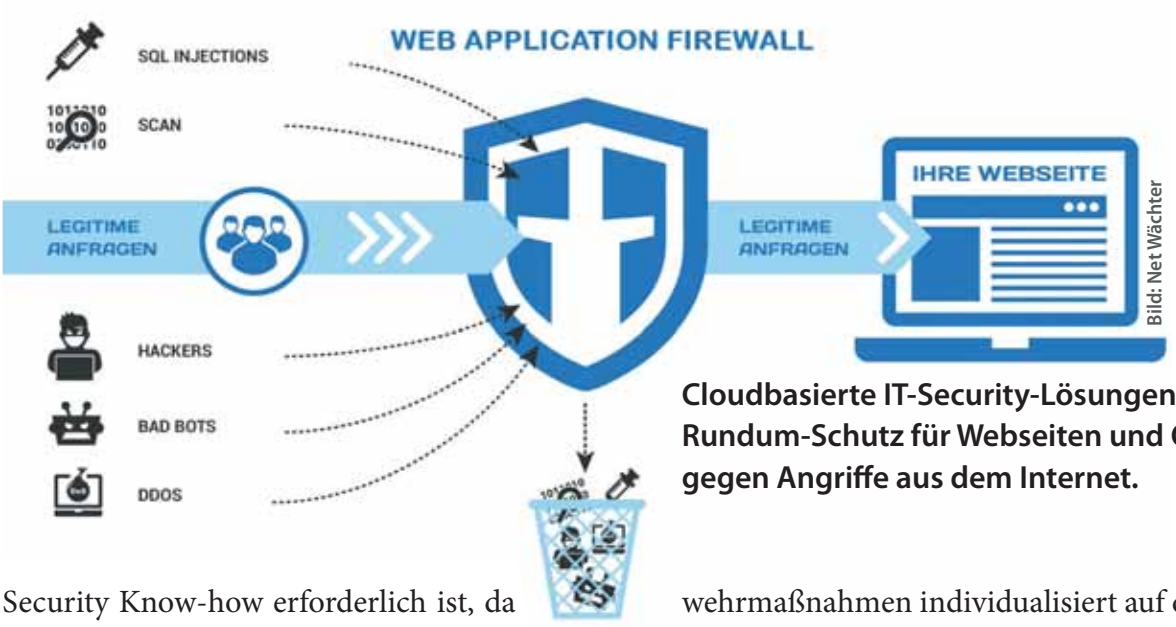
Seit Anfang 2016 steigt die Anzahl an Angriffen mit Cryptotrojanern und neuen Ransomware-Varianten exponentiell. Der Grund: Dies ist leider ein sehr lukratives Geschäft für Cyberkriminelle. Mehr als 1 Milliarde US-Dollar erpressten Hacker damit laut FBI allein im Jahr 2016.
Schlecht gepatchte und ungeschützte Webseiten, die auf bekannten Content-Management-Systemen wie zum Beispiel Wordpress oder Joomla basieren, sind ein leichtes Ziel für Cyberkriminelle und werden so ungewollt zum Verteiler von Spam und Cryptotrojanern. Laut Bitkom rangieren infizierte Webseiten und webbasierte Schadsoftware unter den TOP 3 der Gefahren im Internet.

Gesetzgeber verlangt mehr Sicherheit

Der Gesetzgeber hat das auch erkannt und bereits im Juli 2015 mit der Einführung des neuen IT-Sicherheitsgesetzes die Anforderungen des §13 Abs. 7 Telemediengesetzes angepasst. Alle Gewerbetreibenden sind nun verpflichtet, ihre Webdienste nach aktuellem Stand der Technik zu schützen. Was können nun die Betreiber neben neuen Updates tun, um ihre Webpräsenzen nach aktuellem Stand der Technik zu sichern? Den besten Schutz nach dem aktuellen Stand der Technik bietet momentan nur eine Firewall, die speziell für den Schutz von Web-Anwendungen entwickelt wurde, die sogenannte Web Application Firewall (WAF). Diese schützt die Webseiten und Online-Shops proaktiv gegen Hacker und die Ausnutzung von Sicherheitslücken durch SQL Injections, XSS Forgery, Brute Force oder Schwachstellenscannern.
Insbesondere für kleine und mittlere Unternehmen (KMU) stellt dies eine Herausforderung dar, da sie meistens kein Personal mit IT-Security Know-how haben und auch kein Budget, um teure und komplexe Hardware-WAF-Lösungen zu betreiben und qualifizierte IT-Security Consultants für die Konfiguration und Verwaltung zu bezahlen. Eine cloudbasierte Web Application Firewall kann hier helfen.

Cloudbasierte Web Application Firewalls

Das wichtigste Argument für eine solche cloudbasierte Web Application Firewall, die den KMU „as a Service“ angeboten wird, ist die sehr einfache Konfiguration, für die kein IT-



Cloudbasierte IT-Security-Lösungen bieten einen Rundum-Schutz für Webseiten und Online-Shops gegen Angriffe aus dem Internet.

Security Know-how erforderlich ist, da das Management von einem externen Expertenteam übernommen wird. Lösungen dieser Art werden meist mit Zusatzfunktionen wie DDoS-Schutz, Beschleunigung der Ladezeit, Antivirus – Blacklist-Scans und weiteren Sicherheitskomponenten angeboten. Diese All-in-One Web-Security Suites bieten ein unschlagbares Preis-Leistungs-Verhältnis und können von Unternehmen jeder Größe auch mit kleinerem Budget eingesetzt werden.

Für die Web Application Firewall gibt es zwei grundlegende Architekturen. Zum einen den zentralisierten Ansatz, bei dem die WAF hinter der Netzwerk-Firewall und vor dem Webserver platziert ist, und der gesamte Datenverkehr durch sie hindurch geleitet wird (Reverse-Proxy Mode). Im zweiten Ansatz ist die WAF Host-basiert und als zusätzliche Software direkt auf dem Webserver installiert. Die zentralisierte Architektur stellt üblicherweise höhere Leistungsansprüche, da solche WAFs anders als bei einem dezentralen Konzept meist mehr Anwendungen schützen müssen.

Moderne Web-Application Firewalls werden oft am Anfang im sogenannten „Learning-Mode“ betrieben. In diesem Modus greift die WAF nicht aktiv in den Verkehr ein, sondern beobachtet, wie sich die Applikation und die interagierenden Nutzer verhalten, um die Abwehrmaßnahmen individualisiert auf die jeweilige Anwendung auszurichten und feinzutunen. Auch Anomalien können so später von der WAF besser und schneller erkannt werden.

Für deutsche Unternehmen ist dabei sehr wichtig, hier auf innerdeutsche Lösungen zu setzen, die „made and hosted in Germany“ sind, also den nationalen Gesetzen und insbesondere dem Bundesdatenschutzgesetz unterliegen. Einen vollwertigen WAF-Schutz bietet in Deutschland beispielsweise das Unternehmen Net Wächter (GZIS GmbH) an. Während einer kostenlosen, 14-tägigen Testperiode kann jeder seine Webpräsenz zusätzlich mit einem professionellen Web-Schwachstellenscanner vom weltweit führenden Anbieter Acunetix nach Sicherheitslücken untersuchen lassen. □

Der Autor

Swjatoslav Cicer, CEO und Gründer von Net Wächter (GZIS GmbH), blickt auf über zehn Jahre IT-Erfahrung zurück. Er war zweieinhalb Jahre als IT-Security Consultant beim drittgrößten IT-Systemhaus in Deutschland tätig und verfügt zudem über ein achtjähriges Know-how als IT-Soldat auf Zeit mit Führungsverantwortung.

Sicherer Datenaustausch mit Geschäftspartnern und Kunden

Daten gehören zu den wertvollsten Ressourcen eines Unternehmens – deren reger Austausch mit Geschäftspartnern, Kunden und Kollegen zum modernen Arbeitsalltag. Traditionelle Methoden des Datenaustauschs sind jedoch nicht nur in ihrer Kapazität begrenzt – auch die Sicherheit ist meist in Gefahr. Denn sie bieten keinerlei Kontrollmöglichkeiten über den Zugriff und die Art der Nutzung vertraulicher Dokumente und Informationen. Die Lösung: Virtuelle Datenräume.

NETFILES

Sicherheit, Zuverlässigkeit und Kontrolle – Stichworte, die beim Austausch von vertraulichen Unternehmensdaten oberste Priorität haben. Täglich müssen zahlreiche Dokumente unternehmensübergreifend ausgetauscht werden – per E-Mail, über FTP oder die Cloud. Häufige Folgen: Probleme beim E-Mail-Versand mit Anhängen, kompliziert zu bedienende Software, Kontrollverlust über den aktuellen Stand einer Dokumentversion, Datendiebstahl oder gar Wirtschaftsspionage schädigen das Geschäft.

Virtuelle Datenräume schließen diese essentielle Sicherheitslücke. Unternehmen können mit dieser Lösung ihre sensiblen Daten und Projektunterlagen mit einem Höchstmaß an Sicherheit und Effizienz online austauschen und bereitstellen. Dabei kontrollieren und steuern sie, wer ihre Daten erhält und wie sie genutzt werden dürfen: Ob nur zur Ansicht, zum Download oder zur Bearbeitung.

Bedienkomfort, Kosteneffizienz und Kontrolle der Datensicherheit sind bei der Qualität einer Datenraum-Lösung ebenso wichtige Kriterien wie Seriosität und Standort des Anbieters. netfiles bündelt alle Vorteile: In Deutschland ansässig, unterliegt das Unternehmen den strengen Auflagen des Bundesdatenschutzgesetzes (BDSG). Seine IT-Sicherheitsverfahren wurden vom TÜV Süd nach ISO/IEC 27001 zertifiziert. Im netfiles Datenraum werden sämtliche Dokumente mit dem Advanced Encryption Standard (AES) 256-Bit stark verschlüsselt und vor unbefugtem Zugriff geschützt. Die Server des Anbieters befinden sich ausschließlich in hochsicheren Rechenzentren in Deutschland. Als Software-as-a-Service-Lösung können Unternehmen den netfiles Datenraum ohne aufwändige Schulung oder Bindung von IT-Ressourcen sofort einsetzen. Ein Webbrowser genügt für die Einrichtung und Nutzung der Lösung.

Interessierte Unternehmen können den netfiles Datenraum kostenlos und unverbindlich 14 Tage lang testen:
www.netfiles.de/kostenlos-testen ■

NETFILES

Ihr virtueller Datenraum

Einfach sicher zusammenarbeiten und Daten austauschen

Einfach | Sicher | 15 YEARS Bewährt

Sicherer Datenaustausch

Mit netfiles können Daten einfach und sicher innerhalb eines Unternehmens oder mit Kunden und Lieferanten ausgetauscht und sichere Datenräume für beispielsweise M&A Projekte, Due Diligence Prüfungen, Asset-Transaktionen, Gremienkommunikation, Immobilien- und Vertragsmanagement eingerichtet werden.
Detaillierte Zugriffsrechte regeln Lese- und Schreibrechte im Datenraum und gewährleisten höchsten Schutz bei der Bereitstellung und Verteilung von Dokumenten und eine effektive Zusammenarbeit.

Made in Germany

Höchste Sicherheit für Ihre Daten – Die netfiles GmbH ist ein deutsches Unternehmen mit Sitz, Entwicklung und Hosting in Deutschland.

Jetzt 14 Tage kostenlos testen!

www.netfiles.de

netfiles GmbH Tel. +49 8677 915 96-10 vertrieb@netfiles.de www.netfiles.de

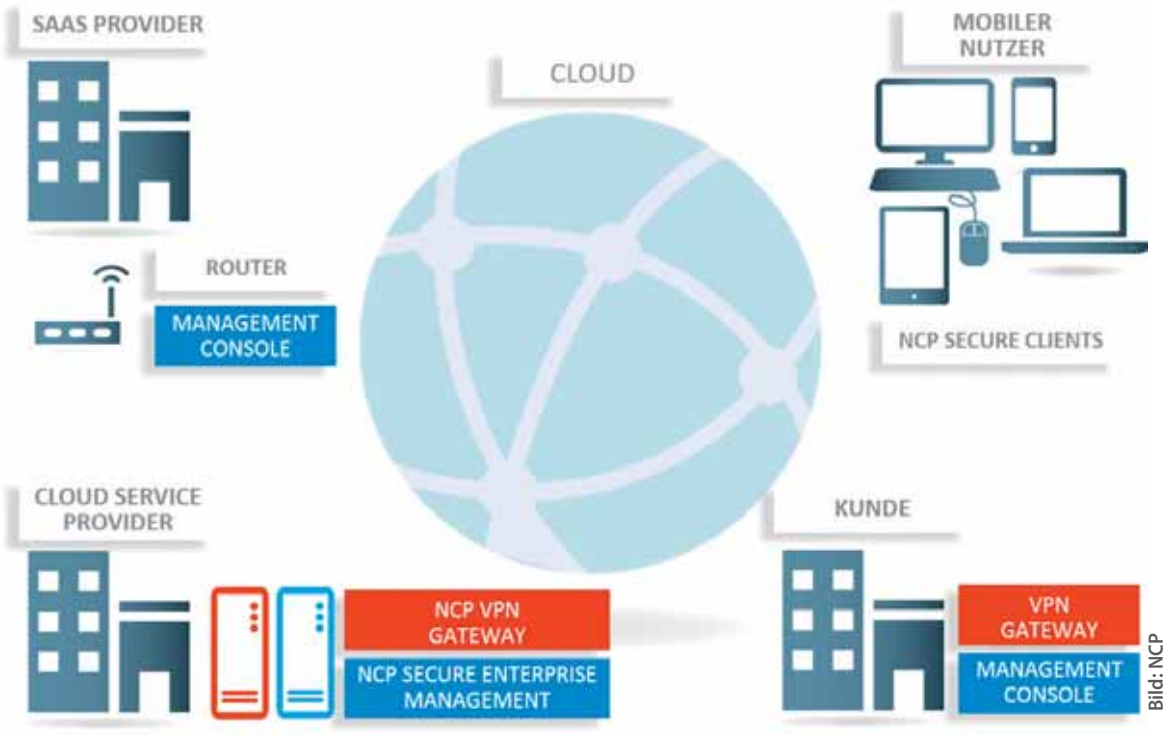
Mehr Remote-Access-Sicherheit durch Cloud-basierte Dienste

Mittlerweile können sicherheitsrelevante Dienste wie Virtual Private Networks problemlos in die Cloud ausgelagert werden. Zahlreiche Anbieter aus den unterschiedlichsten Branchen sind im VPN-Markt aktiv und offerieren ein Komplettangebot, das Kunden im großen Maß an ihre individuellen Ansprüche anpassen können. Von Jürgen Hönig, NCP engineering

Jedes Unternehmen und jedes Netzwerk sind individuell aufgebaut. Doch Dienstleister bieten Managed Security Services wie Virtual Private Network (VPN) schon seit Jahren als Cloud-Dienst an. Dadurch existieren eine große Nutzerbasis und solide Erfahrungswerte, wie ein VPN am besten in die Cloud verlagert werden kann. Wie so oft beginnt die erfolgreiche Implementierung mit dem Sammeln von Daten und Anforderungen. VPN-Betreiber raten übereinstimmend dazu, sich zunächst Gedanken über die Dimensionierung zu machen. Die Anzahl der benötigten Lizenzen ist dabei ebenso relevant wie die Bandbreite der voraussichtlich remote angebundenen Nutzer und Standorte. Welche Netzanbindung dabei genutzt wird, spielt für die Hoster keine Rolle. MPLS wird normalerweise ebenso unterstützt wie der Zugang über IPsec.

Benutzerdaten erfassen und automatisiert verarbeiten

Wichtig ist, sich die Einsatzumgebungen der Clients anzusehen und das Nutzungsszenario zu verstehen. Es geht nicht nur um die Anzahl der Anwender, sondern auch um das Umfeld, in der sie ihre Endgeräte einsetzen. Welche Medien zum Einsatz kommen ist ebenso relevant wie die Frage, ob HotSpots eines gewerblichen Anbieters integriert werden müssen oder ob die Mitarbeiter den Netzzugang auch international benötigen. Die meisten Anbieter haben Fragebögen, mit denen Daten über die dezentrale Infrastruktur gesammelt werden, beispielsweise die Anzahl der Anwender sowie die Art der Endgeräte und die verwendeten Betriebssysteme. Je nach eingesetzter VPN-Lösung sind nicht alle verwendeten Betriebssysteme und Versionen mit den VPN-Clients kompatibel. Wird die verwendete Betriebssystemversion nicht offiziell unterstützt, sollte sie nicht genutzt werden, auch wenn sie bislang funktioniert.
Auf der anderen Seite benötigen die VPN-Dienstleister Angaben über die Art der Einbindung in die Directory- und Metadirectory-Strukturen des Kunden. Bei einer Integration in Active Directory geht es darum zu sehen, wie die Remote-Access-Berechtigungen vergeben sind. Bekommen alle Nutzer Zugang über RAS oder gibt es Gruppen mit unterschiedlichen RAS-Rechten, denen die entsprechenden Nutzer zugeordnet sind? Normalerweise existieren zwei automatisierte Wege, um die Daten vom Kunden zu erhalten. Der Provider kann sich



Mit gehosteten VPNs in der Cloud greifen Kunden bereits auf eine voll funktionsfähige und optimal eingerichtete Lösung zurück. So kommen Organisationen sehr schnell zu einer funktionierenden Sicherheitslösung, die höchsten Ansprüchen gerecht wird.

entweder mit dem Active Directory des Kunden synchronisieren und die entsprechenden Informationen auslesen oder die Daten über eine täglich aus LDAP exportierte CSV-Liste beziehen. Viele Provider bieten auch Sonderlösungen an und können beispielsweise Daten aus der HR-Software entnehmen.

Mehrere Möglichkeiten für Client-Roll-Out

In der Anfangsphase ist die Verteilung der Client-Software die wichtigste Aufgabe. Auch hier sind zwei Varianten denkbar. Gibt es beim Kunden eine Software-Verteil-Lösung, kann der VPN-Client darüber ausgerollt werden. Große Unternehmen verlangen diese Vorgehensweise, weil sie in das Reporting- und Ticketsystem eingebunden ist. Als Alternative bieten manche VPN-Lösungen einen eigenen Verteilmechanismus an. Bei der Lösung von NCP mit dem NCP Secure Enterprise VPN Server (Gateway) ist die Verteilung Bestandteil der Managementplattform NCP Secure Enterprise Management (SEM). In ihr wird lediglich definiert, welche Gruppe das Update erhält. Beim nächsten Anmelden über eine ausreichend schnelle Netzverbindung wird der Client heruntergeladen und installiert. Diese VPN-Lösung kann auch mit jeder anderen Distributionslösung und deren Verteilmechanismus zusammenarbeiten.

Managed-Security-Dienstleistern stehen zahlreiche Produkte und Implementierungsoptionen offen, um einen VPN-Dienst anzubieten. Wichtig ist in jedem Fall, dass die verwendete Lösung und ihre Gateways mandantenfähig sind. So lassen sich unterschiedliche Kunden vollkommen getrennt über physikalische oder virtuelle Systeme bedienen. Durch die hohen Lastanforderungen, die beim Hosting von vielen Tausend VPN-Tunneln entstehen können, ⇨

sollten die Gateways Load-Sharing unterstützen und skalierbar sein. Eine gemeinsame Management-Konsole, die sowohl mit mehreren Gateways pro Kunde als auch mit getrennten Mandanten zurechtkommt, unterstützt die Abläufe der Hoster und die Sicherheitsbedürfnisse der Kunden gleichermaßen. Ob diese ein gemeinsames VPN-Gateway akzeptieren oder eine getrennte Lösung fordern, wird durch ihr jeweiliges Sicherheitskonzept bestimmt. Die VPN-Cloud-Anbieter können in der Regel beide Wünsche erfüllen. Redundante Ausführungen von Gateways und Netzzugängen liegen letztendlich ebenfalls am Anforderungsprofil der Kunden.

Sicherheitsanforderungen bestimmen den Preis

Kunden, die über eine Auslagerung ihrer VPN-Dienste in die Cloud nachdenken, müssen im Vorfeld ihren Schutzbedarf festlegen und die angebotenen Lösungen dahingehend überprüfen. Je nach Risikoprofil können hochqualifizierte Rechenzentren mit Kameraüberwachung, Vereinzelungsschleusen, Vier-Augen-Prinzip und Disaster-Recovery-Spiegelung notwendig sein. Solche Maßnahmen treiben den Preis natürlich in die Höhe. Keine Risiken sollten die Kunden bei der Authentifizierung eingehen. Benutzername und Passwort sind heute nicht mehr ausreichend, ein zweiter Faktor ist für externe Zugänge ins Netz absolut unumgänglich. Zwei-Faktor-Authentifizierung ist Bestandteil einiger VPN-Lösungen. Viele zusätzliche Angebote decken jeden Anwendungsfall ab. So lässt sich ein auf einer Smartcard abgelegtes Zertifikat komfortabel als zweiter Faktor nutzen. Wichtig ist dann, dass der Hoster auch die Zertifikatsverwaltung als Komplettangebot anbietet, so dass eine pünktliche Erneuerung oder der Ablauf der Zertifikate zum Stichtag sichergestellt sind. Unter Umständen sollte es auch möglich sein, weitergehende Authentifizierungsmechanismen einzusetzen, beispielsweise wenn der Remote-Zugang zur Verarbeitung von eingestuftem Material benutzt wird. Schon bei der Sicherheitsstufe VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) fordert das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Einsatz einer zertifizierten Lösung, die zusätzliche Anforderungen an die Authentifizierung und die Unumgehbarkeit des Tunnels stellt.

Zeitaufwand hängt vor allem an administrativen Prozessen

Eine Sicherheitslösung wie ein VPN im Unternehmen einzuführen ist in der Regel mit beträchtlichem Zeitaufwand verbunden. Mit gehosteten VPNs in der Cloud greifen Kunden bereits auf eine voll funktionsfähige und optimal eingerichtete Lösung zurück. Weil die technische Realisierung und die Administration der laufenden Lösung komplett in die Hände des Providers gelegt werden, kommen Organisationen sehr schnell zu einer funktionierenden Sicherheitslösung, die höchsten Ansprüchen gerecht wird. Oft bestimmen eher administrative als technische Prozesse den zeitlichen Ablauf. Die meisten Anbieter rechnen mit einem Zeitaufwand von zwei bis drei Monaten zwischen den ersten Gesprächen und der Realisierung. Wichtig ist es, sich im Vorfeld über das geforderte Sicherheitsniveau, die Anforderungen und Einsatzumgebungen der Clients klar zu werden und für den Cloud-VPN-Provider nachvollziehbar zu dokumentieren. □

Der Autor

Jürgen Hönig ist Leiter Marketing bei der NCP engineering GmbH.

Neue Wege für Datensicherheit in der Cloud

© kran77/stock.adobe.com

In der globalen und digitalisierten Arbeitswelt nimmt das Arbeiten mit Cloud-Lösungen stetig zu. Doch sensible Daten von Unternehmen und Behörden sind in der „Public Cloud" mit herkömmlichen Kontrollen wie z.B. der Passwortabfrage nicht ausreichend vor dem Zugriff Dritter geschützt. Eine Verschlüsselung wiederum erschwert das Arbeiten mit den Dokumenten. Hier braucht es einen völlig neuen Ansatz für die Datensicherheit in der Cloud. Einen Ansatz, der Sicherheit und Transparenz erstmals miteinander verbindet.

Von Dr. Bruno Quint, Rohde & Schwarz Cybersecurity

- Public-Cloud-Dienste wie Dropbox, iCloud oder Google Drive sind nicht mehr nur für Privatanwender relevant. Immer mehr Unternehmen und Behörden arbeiten standortübergreifend mit solchen Cloud-Lösungen und sind auf sie angewiesen. Dabei werden Cloud-Dienste beispielsweise als Plattform für gemeinsames Arbeiten, zur Speicherung von Dokumenten oder für kontinuierliche Backups von Daten genutzt.

Public Clouds geraten jedoch zunehmend ins Visier von Cyberkriminellen. Dadurch entstehen für Unternehmen und Behörden erhebliche Sicherheitsrisiken. Sensible Daten sind nicht immer ausreichend vor fremdem Zugriff geschützt. Der Diebstahl von 68 Millionen Dropbox-Passwörtern durch Hacker im letzten Jahr macht dies deutlich.

Ein weiteres Problem von Cloud-Lösungen: Sicherheitsrelevante und personenbezogene Daten unterliegen strengen Datenschutzvorgaben. Im Zuge der neuen EU-Datenschutz-Grundverordnung (EU-DSGVO) dürfen sensible Daten den Rechtsraum Deutschland nicht verlassen. Die meisten Cloud-Dienste aber haben keine Server in Deutschland und können nicht die entsprechende Datensicherheit garantieren.

Zugriff auf die Cloud und Verschlüsselung der Daten

Daten in der Cloud können auf verschiedene Art und Weise gesichert werden. Grundlegend für die Sicherung ist das Identity und Access Management (IAM). Jede Cloud nutzt solch ein System und regelt den Zugriff über Passwörter, Keys o.ä. Diese können nicht das nötige Sicherheitsniveau gewährleisten. Eine Verschlüsselung der Daten in der Cloud ist deshalb unbedingt nötig. Nur dann können Unternehmen und Behörden ihre sensiblen Dokumente vor fremdem Zugriff schützen.

Herkömmliche Verschlüsselungslösungen schaffen zwar mehr Sicherheit, sie haben aber entscheidende Nachteile: Verschlüsselte Dokumente erschweren das gemeinsame Arbeiten in der Cloud erheblich. Viele Arbeitsprozesse werden dadurch langsam, die Flexibilität der Zusammenarbeit geht verloren. Das ist aber der entscheidende Nutzungs- und Erfolgsfaktor von Cloud-Lösungen.

Neue Sicherheitsstrategien für die Cloud

Eine Alternative sind sogenannte „Cloud Access Security Broker“ (CASB). Der CASB bildet eine neue Kategorie von Cloud-Sicherheitslösungen. Ein CASB befindet sich im Netzwerkverkehr zwischen dem Cloud-Nutzer und dem Cloud-System und kontrolliert alle Zugriffe auf die Cloud. Er regelt sowohl die Authentifizierung der Anwender als auch die Zugriffsrechte auf Dateien und Applikationen in der Cloud. Ein CASB bestimmt beispielsweise die IT-Sicherheitsrichtlinien von Unternehmen für die Nutzeranmeldung, die Protokollierung zum Beispiel von Zugriffen oder die Malware-Erkennung.

Doch obwohl ein CASB die Cloud-Sicherheit erhöht, bietet er keinen ganzheitlichen Schutz. Viele CASB besitzen bspw. kein Verschlüsselungssystem. Sie kontrollieren zwar den Zugriff auf die Daten in der Cloud, die Daten selbst jedoch bleiben unverschlüsselt.

Cloud Access Security Broker mit Verschlüsselung

Soll die Nutzung von Public-Cloud-Diensten zukünftig nicht nur höchsten Anforderungen an die Sicherheit entsprechen, sondern auch die Zusammenarbeit in der Cloud ermöglichen, bedarf es eines neuen Ansatzes: die Verbindung eines Cloud Access Security Brokers mit einem Verschlüsselungssystem von Dateien. Nur eine solche Lösung bietet maximale Sicherheit. Mit diesem „Hochsicherheits-CASB“ können Unternehmen und Behörden sogar mit

hochsensiblen Dokumenten in einer Public Cloud transparent und sicher arbeiten.
Die Lösung arbeitet in mehreren Schritten und schützt mittels Virtualisierung, Verschlüsselung und Fragmentierung Daten selbst vor komplexen Cyberangriffen von innen und außen:
Beim Upload eines Dokuments in die Cloud erstellt der Hochsicherheits-CASB eine virtualisierte Version des Originaldokuments. Dieses virtuelle Dokument enthält nur die Meta-Informationen des Originals, wie Key-Wörter und bestimmte Zugriffsregeln auf das Dokument. Es hat jedoch selbst keinen Inhalt. Das Originaldokument dagegen wird zugleich verschlüsselt und fragmentiert auf unterschiedlichen, frei wählbaren Speichersystemen abgelegt. Diese physikalische Fragmentierung schützt die Daten vor Angriffen und fremden Zugriffen, da das Originaldokument nie vollständig einsehbar ist und nur Fragmente hinterlegt sind. Das erlaubt sogar das Arbeiten mit streng geheimen Dokumenten in der Cloud. Zudem können Unternehmen und Behörden mit diesem CASB ihre Zugriffsrechte auf die Cloud-Dokumente genau definieren und ihre Sicherheitsstrategie für die Cloud umsetzen. Und vor allem: Die hochsensiblen Daten in der Cloud verlassen Deutschland nicht und entsprechen so den strengen Datenschutzvorgaben.
Bei einer erneuten Bearbeitung regelt der Hochsicherheits-CASB den Zugriff auf das Dokument. Ein eigenes Anmeldesystem überprüft über verschiedene Sicherheitsabfragen den Zugriff. Nur Mitarbeiter mit autorisierten Zugriffsrechten können auf das Dokument zugreifen und es herunterladen. Erst beim Download setzt der Hochsicherheits-CASB das Dokument wieder zusammen und entschlüsselt es.
Dadurch bleiben einerseits – selbst bei einem Angriff auf die Cloud – die vertraulichen Inhalte für Angreifer oder nicht befugte Personen unlesbar. Andererseits können Mitarbeiter das Dokument von verschiedenen Standorten aus öffnen und gemeinsam daran arbeiten. Eine mühelose Einbindung in vorhandene Workflows wie Kollaboration, Team-Working etc. ist möglich. Arbeits- und Geschäftsprozesse bleiben erhalten und sind flexibel. Der Hochsicherheits-CASB erlaubt sogar komplexe Arbeitsprozesse wie eine Volltextsuche im verschlüsselten Dokument.

Fazit: Hochsichere und transparente Lösung für die Cloud

Für Unternehmen und Behörden, die hochsensible Dateien in einer Public Cloud teilen und damit arbeiten müssen, reichen herkömmliche Cloud-Lösungen nicht aus. Ein Hochsicherheits-CASB verbindet bisherige Sicherheitslösungen zu einem neuen Ansatz, der einzigartig ist. Durch Verschlüsselung, Virtualisierung und Fragmentierung bietet diese neuartige Cloud-Sicherheitslösung ein Maximum an Datensicherheit, die für den Benutzer zugleich einfach und transparent ist.
Besonders für weltweit tätige Unternehmen und für Behörden mit mehreren Standorten ermöglicht ein Hochsicherheits-CASB flexibles und kollaboratives Arbeiten. Die Lösung ist sowohl beliebig skalierbar als auch mit allen gängigen Cloud-Providern, Fileshare-Systemen und Dateiformaten kompatibel. Damit ist ein Hochsicherheits-CASB nicht nur für große, sondern auch für kleine Unternehmen geeignet. □

Der Autor

Dr. Bruno Quint ist Head of Profitcenter TrustedGate bei Rohde & Schwarz Cybersecurity. Das IT-Sicherheitsunternehmen schützt Unternehmen und öffentliche Institutionen weltweit vor Cyberangriffen.

Sicher, mobil und uneingeschränkt ins Internet

Erfolgreiche Angriffe führen heutzutage meist direkt zur Ausführung von schadhaftem Code im vertrauenswürdigen Unternehmensnetz. Dabei ist die tägliche Bedrohung über das Internet mit herkömmlichen, reaktiven Schutzmaßnahmen wie Virenscannern, funktionalen Einschränkungen oder dem Einsatz von Content-Filtern nicht mehr angemessen in den Griff zu bekommen.

Angesichts des Gefahrenpotenzials dürfte kein einziger Arbeitsplatz einen direkten Internetzugang haben. Zu schnell ist es passiert, dass sich Schadsoftware gewissermaßen beim „vorbeisurfen“ – neben den abgerufenen Nutzinhalten – ihren Weg in das interne Netzwerk bahnt, beispielsweise durch Fremdcontent auf vertrauenswürdigen Internetseiten oder durch den versehentlichen Klick auf den Link in einer Phishing Mail. Andererseits ist die Nutzung des Internets heute an keinem modernen Arbeitsplatz mehr wegzudenken, der Bedarf und das Angebot wertschöpfender Online-Dienste nimmt stetig zu.

secunet safe surfer

Basis von secunet safe surfer ist der Remote Controlled Browser System-Ansatz des Bundesamts für Sicherheit in der Informationstechnik (BSI): Der Internet-Browser wird über sog. Quarantänesysteme angeboten, welche eine vom internen Netzwerk ausgelagerte und gesicherte Zone darstellen. Der Anwender hat von seinem PC aus keinen direkten Zugriff auf das Internet mehr, sondern erhält Bildschirmansichten von seinem ausgelagerten Browser. Diese Trennung sorgt durch einen Medienbruch (Umwandlung der Internetdaten in Bild- und Audiodaten) dafür, dass Schadprogramme weder auf den Anwender-PC noch ins interne Netz gelangen. Zugleich wird eine unzulässige Kommunikation vom PC ins Internet unterbunden. Mit der integrierten Datenschleuse sorgt secunet safe surfer zudem für den sicheren Dateitransfer von Downloads und Druckerzeugnissen ins interne Netz und verhindert unbeabsichtigten Datenabfluss. Die Quarantänesysteme können zentral im Rechenzentrum oder als virtuelle Maschinen (gemäß des Browser-in-the-Box-Prinzips des BSI) auf einem PC oder sogar als Gastsystem auf einer SINA Workstation installiert werden. ■

Ein sicherer Arbeitsplatz.
Wenn er SINA hat.

Die SINA Workstation macht aus jedem Arbeitsplatz einen sicheren Arbeitsplatz – ganz egal, wo er sich befindet. Woran das liegt? An der ausgereiften System-plattform? Ja. An der sicheren Smartcard-Technologie? Auch. Dazu wird Ihre Datensicherheit dank komplett verschlüsselter Dateisysteme und IPsec-geschützter Kommunikation nicht zum Balanceakt zwischen Dürfen, Müssen und Können. Es funktioniert einfach. Immer. Kein Wunder, dass SINA auch höchste Zulassungsanforderungen des BSI, der EU und der NATO erfüllt. Was bedeutet das für Sie? Sie können ganz entspannt darauf vertrauen, dass Ihre Arbeitsplätze dank SINA sicher sind.

IT security „Made in Germany“.
www.secunet.com/sina

secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland

Sicher arbeiten dank Verschlüsselung – fünf Kriterien für Datensicherheit in der Cloud

Die Auslagerung von Geschäftsprozessen und Informationen in die Cloud ist ein verlockender Weg, um Ressourcen einzusparen und die Produktivität bequem zu sichern – oder die Verantwortlichkeit dafür in andere Hände zu legen. Doch der Königsweg für den IT-Administrator ist für CDOs oder CISOs, die den Datenschutz in der Cloud verantworten, ein Tanz auf dem Seil ohne Netz. Verschlüsselung spannt dieses Netz.

Von Elmar Eperiesi-Beck, eperi

Weil ab Mai 2018 die Europäische Datenschutzgrundverordnung (EU-DSGVO) verbindlich die rechtlichen Rahmenbedingungen für den Datenschutz und damit die Anforderungen an Datensicherheit auch in der Cloud festlegt, wird Verschlüsselung als effektivste Verteidigungslinie zum Schutz der Informationen gerade in der Cloud immer wichtiger. Aber Verschlüsselung ist nicht gleich Verschlüsselung. Wirkliche Sicherheit hängt von fünf zentralen Kriterien ab.

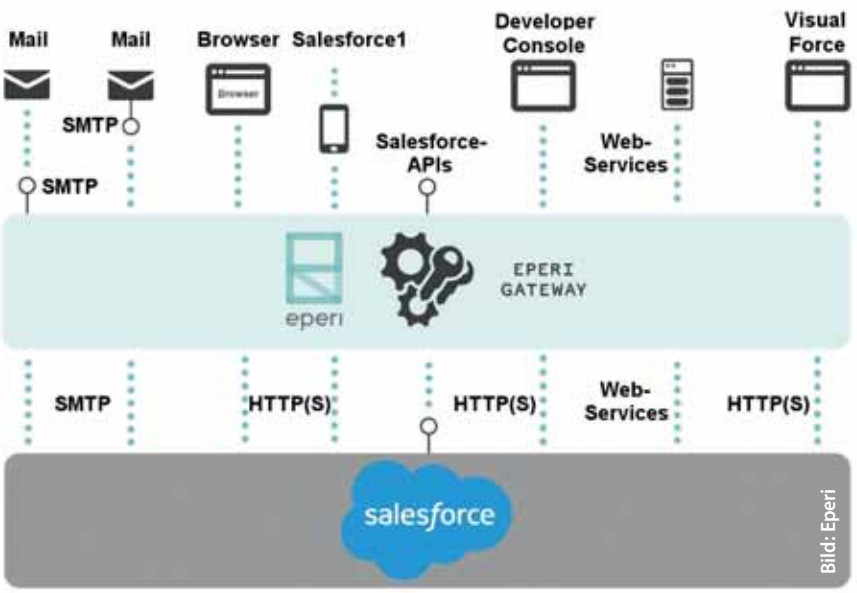
Kriterium 1: Verschlüsselung überall, jederzeit und korrekt

Nur eine Datenverschlüsselung verschlüsselt, im Gegensatz zur Transportverschlüsselung, Daten an jedem Speicherort und zu jedem Zeitpunkt. Erst ein solches Verfahren bietet höchstmögliche Sicherheit. Denn jeder Ort oder jede Anwendung, an dem Daten im Klartext zugänglich gemacht werden, wird zur Sicherheitslücke. Gerade bei in der Cloud gespeicherten Daten kommt es auf die lückenlose Verschlüsselung an. Sicher sind Informationen nur dann, wenn sie mathematisch korrekt und vollständig verschlüsselt werden. Verfahren zur Teilverschlüsselung, die oft benutzt werden, um Informationen in den verschlüsselten Daten zu suchen oder sortieren zu können, lassen sich leicht aushebeln. Dieser schwerwiegende Sicherheitsmangel lässt sich aber vermeiden, ohne auf diese Funktionalitäten zu verzichten.

Kriterium 2: Keine Einschränkungen bei der Produktivität

Die Unterstützung von Anwendungen muss nicht auf Kosten der Datensicherheit gehen. Gateway-basierte Verfahren unterstützen berechtigte Anwender bei ihrer Arbeit mit den Daten – ohne Verlust von Funktionalitäten. Bei Datenverschlüsselungen gewährleisten Funktionalitätsemulationen, die nur den berechtigten Anwendern über eine Applikation wie ein Gateway bereitstehen, die Arbeit mit Datenbeständen, als ob es keine Verschlüsselung gäbe.
Auch Tokenisierungsverfahren ermöglichen es berechtigten Anwendern, mit Daten zu arbei-

ten, die nur sie im Klartext sehen. Anderen aber werden nur Ersatzwerte dargestellt. Zur Tokenisierung der Informationen generiert ein Gateway für jeden Datensatz typkonforme Werte. So wird gewährleistet, dass Anwendungs-Workflows weiter funktionieren und nur der Ersatzwert in der Cloud gespeichert wird. Für die Datensicherheit ist aber eine sichere Tokenization wichtig. Bei älteren Verfahren sind typkonforme Ersatzwerte oft in einer Mapping-Tabelle verzeichnet, welche daher ein beliebtes Ziel für Hacking-Angriffe ist. Wichtig ist es daher, die Originaldaten vor Eintragung in die Token-Tabelle zu verschlüsseln und starke Verschlüsselungen und Tokenization zu kombinieren.



Arbeiten mit verschlüsselten Daten: Ein Verschlüsselungsgateway ermöglicht dem berechtigten Anwender den sicheren Zugriff auf und das Arbeiten mit verschlüsselten Anwendungsdaten, unabhängig von der Zugriffsart.

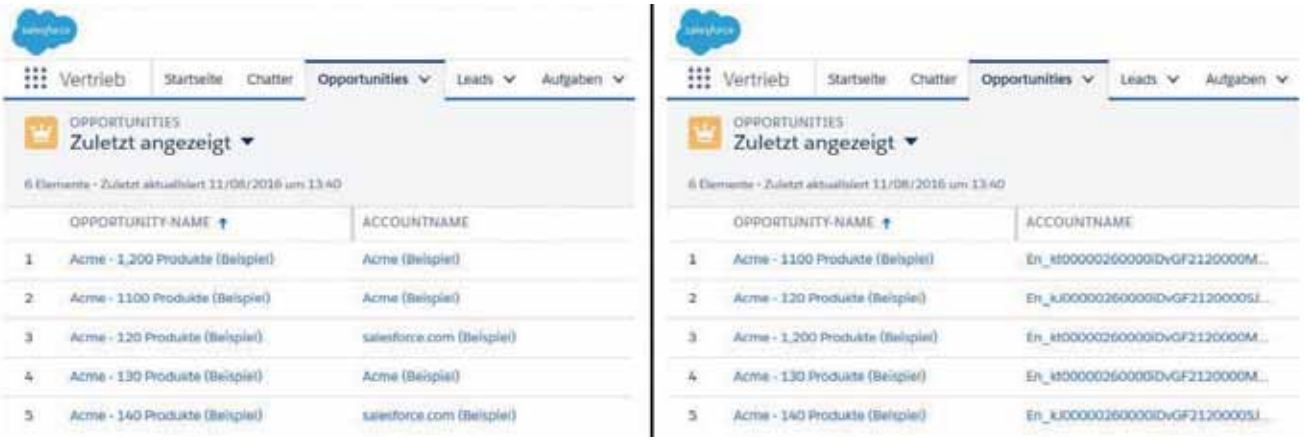
Kriterium 3: Datensicherheit schnell verwirklichen

Verschlüsselungslösungen müssen schnell für Sicherheit sorgen, ohne die bestehende IT-Infrastruktur zu verändern und damit die Funktionalität von Anwendungen zu beeinträchtigen. Eine schnelle Implementierung spart Geld. Letztlich lässt sich oft auch nur so die Anschaffung einer solchen Lösung im Unternehmen durchsetzen. Eine Gateway-Struktur, die vor die eigentliche IT-Infrastruktur geschaltet wird, die Verschlüsselung samt Funktionsemulation außerhalb einer zu schützenden Anwendung durchführt und dem unberechtigten Anwender immer nur verschlüsselte tokenisierte Daten präsentiert, bietet nicht nur Sicherheit. Sie macht es auch möglich, dass bestehende Infrastrukturen nicht geändert werden müssen und Verschlüsselungen schnell implementiert werden können. Und wenn Anwender bestimmen können, welche Daten nur verschlüsselt werden müssen – also etwa personenbezogene Daten, aber nicht Patientendaten – und das Gateway seine Rechenleistung zur Verarbeitung von Suchanfragen einbringt, kommt es auch zu keinen nennenswerten Performance-Verlusten.

Kriterium 4: Klare Verantwortlichkeiten – insbesondere beim Gang in die Cloud

Datensicherheit erfordert eine konsequente Regelung und Gewaltenteilung der Zugriffsrechte auf Schlüssel und Daten. Bei sicheren Lösungen bleibt die Generierung und Verwaltung individueller Schlüssel ohne Wenn und Aber im eigenen Unternehmen. Hersteller der Verschlüsselungslösung oder der Applikation oder auch Betreiber von Cloud-Rechenzentren bleiben außen vor. Anfragen Dritter zur Herausgabe der Schlüssel oder zur Entschlüsselung an Externe sind also zwecklos.

Aber auch unternehmensintern sollte sich der Kreis der Schlüsselverwalter so klein wie möglich halten lassen. Am besten verwaltet nur ein ausgewählter Sicherheitsadministrator ⇨



Ohne das Gateway sieht der Nutzer nur verschlüsselte Daten (rechts). Berechtigte erhalten über das Gateway Zugriff auf die Klartextdaten (links) ohne Änderung der Benutzeroberfläche.

die Schlüssel. Dieser kann Schlüssel lediglich zuteilen und entziehen, ohne je auf Daten im Klartext zugreifen zu können. Der Zugriff auf die verschlüsselten Daten ermöglicht ihm aber deren administrative Bearbeitung – wie Kopieren, Verschieben oder das Veranlassen von Backups, Spiegelung oder Migration. Für den Datenzugriff hängt der berechtigte Benutzer von der Verwaltung seiner Rechte durch den IT-Administrator, beispielsweise über ein Meta Directory, ab. Die Rechtevergabe erfolgt in der Applikation, die die Daten verschlüsselt, also etwa in Salesforce oder Outlook 365.

Kriterium 5: Compliance

Eine Verschlüsselungslösung hilft auch Unternehmen bei der Erfüllung der immer weiter zunehmenden Anforderungen des Datenschutzes. Dieses Problem drängt angesichts der bevorstehenden Verschärfungen bestehender Datenschutzgesetze und neuer Vorschriften, wie die NIS-Richtlinie oder die EU-DSGVO/GDPR, immer mehr. Verschlüsselung löst offensichtlich alle Probleme, denn sie macht Daten in jedem Fall unbenutzbar weil unlesbar. Richtige Verschlüsselungsimplementierung dokumentiert die Anstrengungen zur Pseudonymisierung oder Verschlüsselung persönlicher Daten (laut Artikel 32 der EU General Data Protection Regulation 2016/679 – GDPR), hilft bei Erfüllung der Forderung nach Auswahl geeigneter Schutztechnologien (Artikel 25 GDPR), nach administrativer Verwaltung des Zugangs durch Nutzerrechte (Artikel 32 GDPR), nach Minimisierung der Datenverarbeitung (Artikel 5 GDPR), wenn etwa nur für Dritte wertlose verschlüsselte Werte das Unternehmen verlassen, oder auch nach Zentralisierung des Datenschutzes (Recital 36 GDPR). □

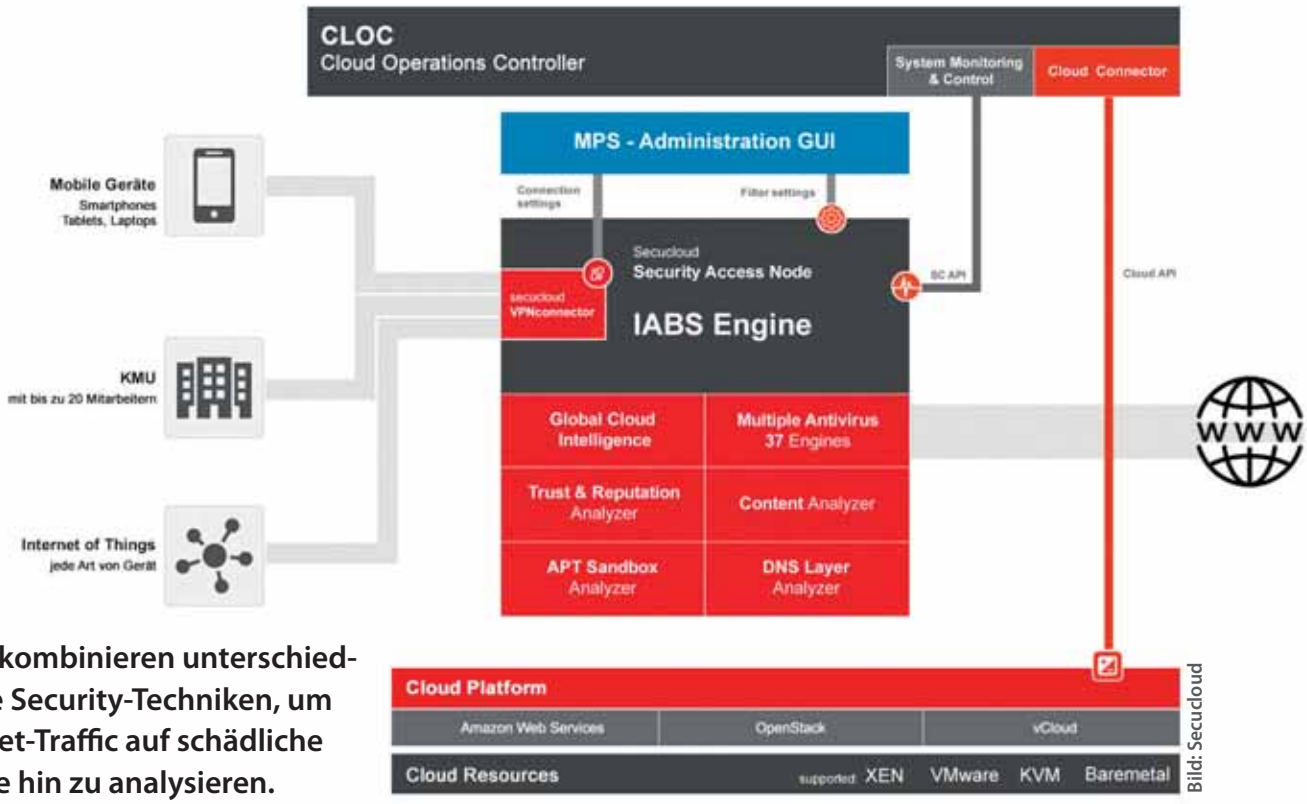
Der Autor

Elmar Eperiesi-Beck ist Geschäftsführer und Gründer des IT-Security-Spezialisten eperi GmbH. Nach seinem Studium der Wirtschaftsinformatik war er bei IBM Global Services als Prinzipal tätig, bevor er 2003 eperi gründete. Mit seinem Team und starken Partnern wie IBM, Microsoft, Salesforce, SAP und T-Systems hilft er seit 10+ Jahren mehreren 100 internationalen Enterprise-Kunden dabei, Daten in Datenbanken und Cloud-Anwendungen zuverlässig und sicher zu verschlüsseln.

Managed Security Services: Nicht länger Privileg der Großen

Digitalisierung sei Dank: Auch kleine Unternehmen profitieren heutzutage im gleichen Maße wie große Konzerne von flexiblen Cloud-Services – gleichzeitig verfügen sie jedoch nicht über die Ressourcen, ihre Internet-Nutzung ebenso gut gegen Hacker und Cyberkriminelle abzusichern. Ein Umdenken bei den Security-Anbietern ist daher unerlässlich: Cloud-basierte Managed Security Services müssen stärker auf die Anforderungen kleiner Unternehmen zugeschnitten werden.

Von Felix Blank, Secucloud



MSSP kombinieren unterschiedlichste Security-Techniken, um Internet-Traffic auf schädliche Inhalte hin zu analysieren.

Allzu lange ist es gar nicht her, da zeichnete sich das Internet vor allem durch seine asymmetrischen, langsamen Verbindungen aus und diente in erster Linie Unterhaltungszwecken. Im vergangenen Jahrzehnt hat sich dies grundlegend verändert. Heute bewegen sich Bandbreiten im Gigabit-Bereich, und für viele Unternehmen ist das Internet nicht mehr nur Kommunikationsweg oder externe Informationsquelle. Dank Cloud Computing und Software-as-a-Service- ⇨

Angeboten ist das Internet längst zur Rechner- und Speicherinfrastruktur der Unternehmen geworden: Services und Daten verbleiben in der Cloud und werden nicht mehr lokal genutzt.
Ein Trend, der längst nicht nur die großen Konzerne betrifft: Selbst kleinste Unternehmen wie Anwaltskanzleien oder Arztpraxen sind heutzutage ohne Internet nicht mehr in der Lage, ihrem Tagesgeschäft nachzugehen. Entsprechend ist die Anzahl der internetfähigen Geräte exponentiell gewachsen – und damit die Anzahl der potenziellen Einfallstore für Cyberkriminelle.

Schöne neue Online-Welt

Und in der Tat sind gerade Daten in der Cloud ein besonders lukratives Ziel für Cyberkriminelle und Hacker. So lässt sich gerade in den vergangenen Jahren auch ein Wandel in der Bedrohungslage erkennen: DDoS-Angriffe per Botnetz, Phishingangriffe oder Datenklau werden heutzutage auf hochprofessionellem Niveau vorbereitet und durchgeführt. Hinter den Attacken stehen längst nicht mehr nur die berühmt-berüchtigten Scriptkiddies oder einzelne Hacker. Hinter den Bedrohungen der heutigen Zeit stehen handfeste wirtschaftliche Interessen, so dass sich das Geschäft mit Cyberangriffen und Malware zu einem professionellen Gewerbe weiterentwickelt hat.
Während moderne Sicherheitstechnologien wie Intrusion-Detection-/Intrusion-Prevention-Systeme (IDS/IPS), Gateway-Antivirus, URL- und Content-Filter oder VPN in Enterprise-Netzwerken längst zum Standard geworden sind, können sich kleine und mittelständische Unternehmen diese teuren Spezial-Appliances oft nicht leisten. Ein fatales Dilemma: Denn mit der zunehmenden Etablierung von Cloud- und Internetdiensten in kleinen Unternehmen steigt auch deren Attraktivität für Cyberkriminelle – nicht zuletzt dank des unzureichenden Schutzniveaus, das Hacker dort vermuten und in vielen Fällen auch tatsächlich vorfinden.

Bild: Secucloud

Die Firewall-as-a-Service schützt die Unternehmensinfrastruktur bereits in der Cloud.

Unified Threat Management erleichtert Sicherheit im Mittelstand

Abhilfe für kleine und mittlere Unternehmen versprach in der Vergangenheit vor allem das sogenannte Unified Threat Management (UTM), in gewisser Weise die natürliche Weiterentwicklung der traditionellen Firewall. Dabei geht das Funktionsspektrum der UTM-Appliances jedoch weit darüber hinaus: Sie vereinen unterschiedlichste Security-Funktionen in einer einzigen Appliance.
Verkauft werden diese meist durch lokale Netzwerkintegratoren, die als Reseller für ein oder zwei UTM-Hersteller lizenziert sind. Sie richten die entsprechenden IT-Security-Funktionalitäten für kleine und mittelständische Unternehmen ein, betreiben und pflegen diese im Anschluss und kümmern sich bei Bedarf auch um deren Support. Der Vorteil eines solchen Ansatzes liegt auf der Hand: Die Security-Techniken lassen sich zentral bedienen und überwachen, und auch weniger IT-Security-erfahrene Administratoren sind so in der Lage, bestmöglich für den Schutz des Unternehmens zu sorgen.

IT aus der Cloud braucht Security aus der Cloud

Doch gerade für kleine Unternehmen mit weniger als 20 Mitarbeitern ist ein solcher verwalteter Security-Service häufig zu kostenintensiv. So ist für sie eine neue Herangehensweise an eine zentralisierte Sicherheitsinfrastruktur gefragt, die explizit auf die Anforderungen kleiner Unternehmen zugeschnitten ist. Ein möglicher Lösungsansatz könnte sich hierbei in der Cloud finden: ein remote-betreuter Firewall-Cloud-Service, für den das Analystenhaus Gartner kürzlich den Begriff der „Firewall-as-a-Service" als neue Kategorie definiert hat.

Ein solcher Service bringt die Vorteile der Cloud auch in die IT-Security: Er ist immer aktuell, skaliert bei höheren Anforderungen automatisch und arbeitet auch bei leistungsintensiven Security-Filtern ohne Performancebeeinträchtigungen. Die benötigten Security-Profile sind vordefiniert und werden direkt vom Anbieter sichergestellt. Auf diese Weise macht er High-Security-Features aus dem Enterprise-Umfeld auch für kleinere Unternehmen uneingeschränkt verfügbar. Ein zentraler Vorteil, da gerade kleine UTM-Lösungen durch ihre Hardware in der Performance beschränkt sind. Angeboten werden solche „Firewall-as-a-Service"-Lösungen von Managed-Security-Service-Providern (MSSP), die das externe Managen und Monitoren der IT-Security im Unternehmen übernehmen.

Spezialisierte MSSP für kleine Unternehmen

Bislang zielt jedoch auch ein solcher Service häufig hauptsächlich auf mittelständische Unternehmen ab. Neben den etablierten muss daher eine neue Generation Managed Security Services für kleine Unternehmen entstehen, deren Angebot sowohl preislich als auch vom Funktionsumfang her auf die Bedürfnisse kleiner Unternehmen zugeschnitten ist. Eine entsprechende Weiterentwicklung der Netzwerkintegratoren ist in Zeiten der allumfassenden Digitalisierung unerlässlich.

Bei Managed Security Services für kleine Unternehmen wird der Kundenbetreuer, der in der Vergangenheit die Sicherheitsinfrastruktur seiner Kunden vor Ort betreute, nun zusätzlich durch die vom Anbieter zur Verfügung gestellte IT-Security-Plattform unterstützt. Diese verfügt dank cloudbasierter IT-Security-Infrastruktur über einen Echtzeit-Überblick der aktuellen globalen Bedrohungslagen und ist so in der Lage, bei neuen Gefahren und Angriffswellen sofort mit gezielten Maßnahmen aus der Cloud zu reagieren. Für den MSSP selbst bringt ein solches Konzept ebenfalls Vorteile: Er ist in der Lage, deutlich mehr Kunden zu betreuen, als dies im Rahmen des traditionellen Ansatzes möglich wäre, und so sein Geschäftsmodell in Zeiten der Digitalisierung zu optimieren.

Aktuell liefern bereits mehrere Anbieter entsprechende Firewall-as-a-Services auch zum Weiterverkauf für Reseller. Hier hat sich u.a. Secucloud spezialisiert und bietet den neuen MSSP für kleine Unternehmen eine vollständige Kunden-, Lizenz und Support-Verwaltung, die diese unter eigenem Logo vertreiben können. □

Der Autor

Felix Blank ist Senior Product Manager beim deutschen Security-Spezialisten Secucloud. In seiner Position betreut er sowohl die Entwicklung und die Vermarktung der Produkte als auch die innovativen Forschungen im Bereich Cloud Security und KI. Als Anbieter von cloudbasierten Sicherheitslösungen ermöglicht Secucloud seinen Kunden auf Basis seines leistungsstarken „Elastic Cloud Security System" (ECS²) ein Sicherheitsniveau nach Industriestandard.

Mobiles Arbeiten – einfach und sicher!

Mobile Technologien treiben die digitale Transformation voran. Unternehmen wollen die Potenziale dieser Technologien ausschöpfen, müssen sich aber auch der Risiken bewusstwerden. Je mehr auf mobilen Geräten gearbeitet wird, desto interessanter werden diese für Angreifer.

SecurePIM – das „Office To Go“

SecurePIM ist eine schlanke Lösung für Unternehmen mit hohen Ansprüchen an Datensicherheit und Datenschutz. Alle Arbeitsvorgänge und die dazugehörigen Daten sind in einer sicheren Container-App auf dem mobilen Endgerät geschützt. Data Leakage und Fehlverhalten des Mitarbeiters ist damit ein Riegel vorgeschoben. Im Container befinden sich die üblichen „Outlook-Funktionen“ wie E-Mail, Kontakte, Kalender, Aufgaben sowie ein einfacher Zugriff auf Dateien und deren Bearbeitung, Internetzugriff, z.B. für Intranet-Anwendungen, und eine sichere Kamera.

Sicherheit für alle Fälle

Die hoch sichere App für mobiles Arbeiten ist einfach zu installieren und fügt sich problemlos in existierende Infrastrukturen ein. Ob iOS oder Android – SecurePIM ist für beide Systeme verfügbar und ist genau so einfach zu bedienen, wie bekannte Apps auf den jeweiligen Geräten. So können Unternehmen ganz einfach ihre Daten und die Privatsphäre der Mitarbeiter und Kunden schützen. Nur Sicherheit, die den Nutzer nicht einschränkt, wird sich durchsetzen.

Sicherheit auf höchstem Niveau

Bei der Entwicklung von SecurePIM wurde eng mit dem BSI zusammengearbeitet und die Systemlösung SecurePIM Government SDS ist vom BSI für die Datenkommunikation bis zur Sicherheitsstufe „Verschlusssache – nur für den Dienstgebrauch“ (VS-NfD) zugelassen. Dies unterstreicht den hohen Sicherheitsanspruch, den Virtual Solution an seine Produkte hat. ■

Die Business App

iOS

OFFICE TO GO

Die einfachste und sicherste
Möglichkeit, mobil zu arbeiten.

SecurePIM Office

IT-SICHERHEIT MADE IN GERMANY. SECUREPIM.COM

Mehr IT-Sicherheit für den deutschen Mittelstand

Die IT-Sicherheit im deutschen Mittelstand ist auf erschreckend niedrigem Niveau. Entscheider in den Unternehmen sind noch immer der Meinung, dass Kauf und Installation einer hochwertigen Sicherheitslösung sofort alle Probleme lösen würde. Aktuelle Studien zeigen, dass dies jedoch nur in den seltensten Fällen der Realität entspricht. Effektive IT-Sicherheit ist ein kontinuierlicher und konsequent entwickelter Management-Prozess, welcher unter dem Namen Managed Security Service firmiert. Von Eric Kaiser, Securepoint

Anhand eines Beispiels soll verdeutlicht werden, welchen Stellenwert der Managed Security Service einnimmt und welch horrende Probleme durch einen Verzicht auf eine moderne und dauerhafte Lösung entstehen können. Im nun folgenden Beispiel wurden alle Namen anonymisiert, um Rückschlüsse auf das Unternehmen vermeiden zu können.

IT-Sicherheit auf vielen Ebenen

Peter Maier, Geschäftsführer eines führenden deutschen Unternehmens für Klimatechnik, wurde von seiner Buchhalterin Martina Frei über einen Anruf der Bank unterrichtet. Annähernd 450.000 Euro seien auf ein falsches Konto überwiesen worden. Das Geld sei nicht auf dem Konto des neuen asiatischen Geschäftspartners eingegangen, sondern auf ein bisher unbekanntes Drittkonto überwiesen worden. Nach Prüfung der Bank sei davon auszugehen, dass es keinerlei Möglichkeit für das Unternehmen gäbe, das Geld wieder zu erlangen.

Umgehend wurde eine Überprüfung der IT-Sicherheit angeordnet. In einem Telefongespräch bestätigte der Leiter der IT, Herr Wolfgang Urbach, dass die Sicherheitssysteme des Unternehmens auf dem neuesten Stand seien. Das Unternehmen hatte erst vor zwei Jahren einen fünfstelligen Betrag in den Kauf einer neuen IT-Sicherheitslösung investiert und diese durch kompetente Fachfirmen einrichten lassen. Als nächster Schritt sollte zunächst eine umfassende Analyse mit dem amerikanischen Hersteller der Sicherheitslösung durchgeführt und eine Strafanzeige gegen Unbekannt gestellt werden. Ein IT-Forensiker wurde hinzugezogen.

Nach zwei Monaten standen die ersten Ergebnisse fest. Die Kriminalpolizei konnte bestätigen, dass der überwiesene Betrag bereits abgehoben war und nicht mehr rückverfolgt werden konnte.

Oliver Schönleben, der IT-Forensiker, konnte darüber hinaus aufklären, wie es zu der verhängnisvollen Überweisung gekommen war.

Der Grund sei kein technisches Versagen der Firewall, sondern ein Fehler in den Betriebsabläufen des Unternehmens. Eine unbekannte Person hatte es geschafft, den Mailverkehr des Absenders so zu manipulieren, dass eine falsche Kontonummer in den E-Mail-Verkehr eingeschleust werden konnte. Der Fehler lag zum einen im Bereich der Buchhaltung, welche sich telefonisch beim neuen Partner die Korrektheit der Kontonummer hätte bestätigen lassen müssen. Zum anderen hätte durch die Verwendung von signierten E-Mails auch technisch das Risiko manipulierter E-Mails deutlich reduziert werden können.

IT-Sicherheit als Prozess

Herr Schönleben erklärte Herrn Maier, dass sein Unternehmen in Zukunft die IT-Sicherheit als Management-Prozess etablieren müsste, und dass es nicht genüge, sich allein auf die technischen Sicherheitssysteme zu verlassen. Es müssen in einem beständigen Prozess die aktuelle Gefahrenlage geprüft und die notwendigen Maßnahmen ergriffen werden.

Die größte Schwachstelle des Unternehmens sei bei der IT-Sicherheit nicht bedacht worden: die Mitarbeiter. Denn diese sind in den meisten Fällen die Haupt-Angriffsziele der Kriminellen und dementsprechend muss hier die Sicherheit besonders hoch bewertet werden.

Herr Schönleben und Herr Urbach entwickelten gemeinsam eine Liste von Elementen und Maßnahmen, welche von diesem Zeitpunkt an regelmäßig überprüft und durchgeführt werden sollten.

Hierzu gehörten unter anderem:

- Die regelmäßige Schulung und Sensibilisierung von Mitarbeitern
- Die Sicherheitssysteme beständig aktuell zu halten (Updates, Konfigurationen usw.)
- Der konsequente Einsatz der technischen Sicherheitssysteme auf allen Ebenen (Zugriffsrechte, Filter, GPOs)
- Bewertung aktueller Gefahren und daraus resultierende neue Maßnahmen
- Die Umsetzung der grundlegenden Regeln für die betriebliche IT-Sicherheit

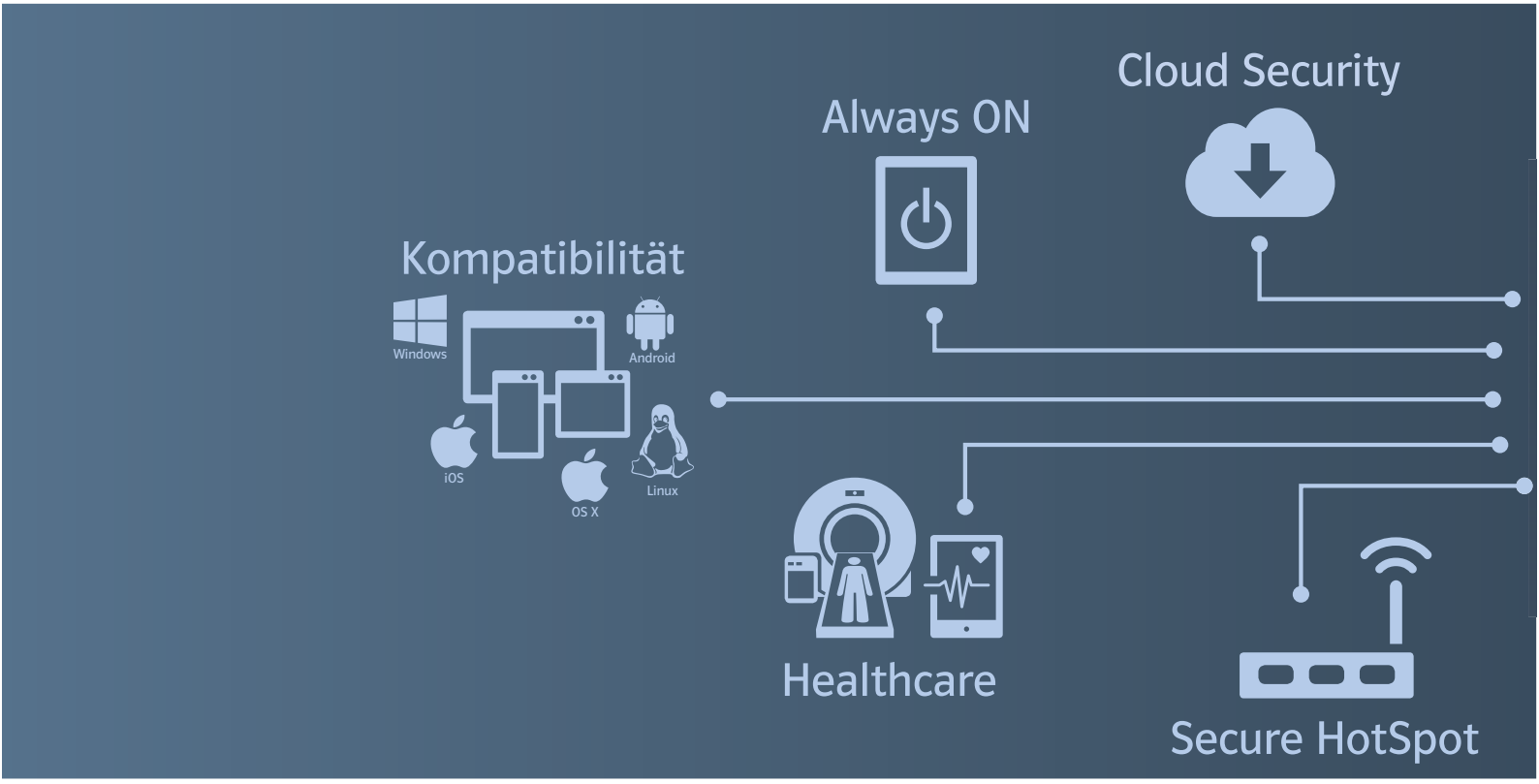
Grundlegende Regeln

- IT-Sicherheit ist Verantwortung der Unternehmensleitung
- Jeder Mitarbeiter darf nur genau auf das zugreifen, was er auch zum Arbeiten benötigt
- Alle Sicherheitsmaßnahmen gelten für alle Hierarchiestufen – ohne Ausnahme

Um die Einführung des Managed Security Service im Unternehmen zu vereinfachen und zu etablieren, suchte sich Herr Urbach Unterstützung bei einem Systemhaus und einem deutschen IT-Sicherheitsunternehmen und sicherte sich somit die notwendige Manpower und das benötigte Know-how. Die Unternehmensleitung um Herrn Maier hat diese Kosten bereitwillig übernommen, da diese Investition sich dauerhaft auf die Sicherheit des eigenen Unternehmens auswirkt und somit für mehr Sicherheit Sorge trägt. □

Der Autor

Eric Kaiser ist Produktmanager beim deutschen IT-Security Spezialisten der Securepoint GmbH aus Lüneburg. Ursprünglich aus dem Systemhausgeschäft kommend, kennt er die Anforderungen bei der Einführung von IT-Security bei Kunden. Bei Securepoint ist er verantwortlich für das gesamte Produktportfolio vom NextGen UTM-Firewalls über E-Mail-Archivierung bis Antivirus Pro. Des Weiteren entwickelt er Lösungen wie „Security as a Service" für den Cloud-Bereich und Weiterbildungen für Managed Security.



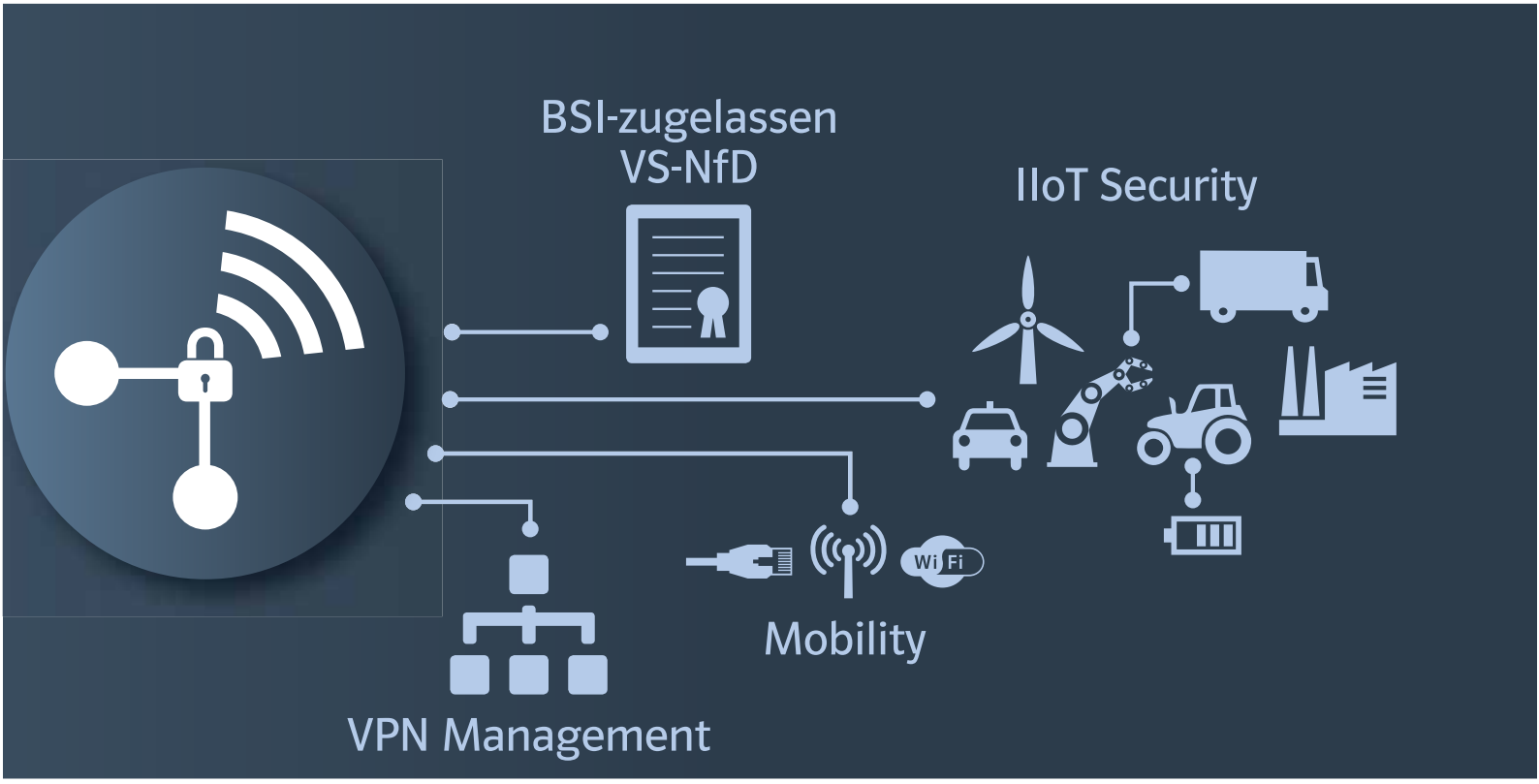
Grenzenlose Daten

#EINFACH #MANAGEBAR #FLEXIBEL #SICHER

Jetzt informieren!

Sicherheit made in Germany

NCP
SECURE COMMUNICATIONS



schnelle &
Zero Touch Konfiguration einfache Rollouts

kommunikation

Zertifikats zentrales
management Management

Industrie 4.0 Sicherheit softwarebasiert

plattformfähig cloudfähig

Secur IT y
made in Germany

Fünf Pfeiler sicherer Verschlüsselung

Tagtäglich werden unzählige Datenströme über das Internet verschickt. Der Großteil davon unverschlüsselt, ein gewisser Anteil auch mit verschiedenen Methoden verschlüsselt. Im Folgenden soll erläutert werden, welche fünf Eigenschaften eine nach dem Stand der Technik sichere Verschlüsselung ausmachen und wie die Einhaltung dieser Prinzipien gewährleistet wird.

Von Markus Schräder, CryptoMagic

Authentifizierung

Das Ziel einer sicheren Authentifizierung ist es zu gewährleisten, dass die Kommunikation nur mit dem Kommunikationspartner stattfindet, mit dem sie erfolgen soll. Auch bei einer korrekt durchgeführten Verschlüsselung besteht die Gefahr, mit der falschen Gegenstelle zu kommunizieren: In diesem Fall würden die Informationen zwar sicher verschlüsselt übertragen, aber dennoch in die falschen Hände geraten. Eine weitere Angriffsmöglichkeit sind Man-in-the-middle-Angriffe, bei denen sich der Angreifer unbemerkt zwischen die Kommunikationspartner schaltet und deren Kommunikation mitlesen und manipulieren kann.

© Jakub Jirsák/stock.adobe.com

Im Bereich der Computerkryptographie nutzt man zum Schutz hiervor üblicherweise Software-Zertifikate, die auf Methoden der asymmetrischen Verschlüsselung sowie des Hashings (d.h. der Fingerabdruck des Zertifikats) beruhen: Diese Zertifikate können genutzt werden, um der jeweiligen Gegenstelle zu beweisen, dass sie mit dem System kommuniziert, mit dem sie denkt zu kommunizieren. Die Wirkungsweise ist mit dem Vorzeigen eines Personalausweises vergleichbar, wodurch Sie die Identität Ihres Gegenübers sicher feststellen können.

Verschlüsselungsverfahren

Das Verschlüsselungsverfahren dient dazu, mit mathematischen Methoden einen Datenstrom unter Anwendung eines sogenannten Schlüssels so umzuwandeln, dass auf den ursprünglichen Klartext nur noch mit dem Schlüssel zugegriffen werden kann. Hierbei wird zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden:

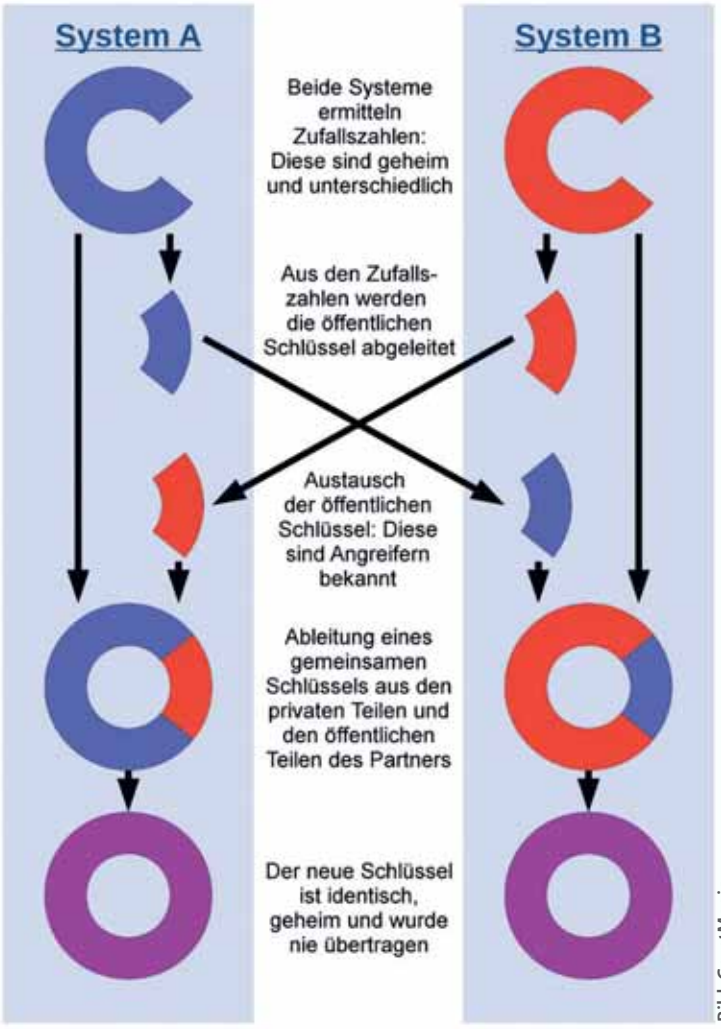
Symmetrische Verfahren besitzen einen Schlüssel, der beiden Kommunikationspartnern bekannt sein muss, da dieser sowohl der Ver- als auch der Entschlüsselung dient. Ein komplexes Problem hierbei ist, beiden Partnern denselben Schlüssel zukommen zu lassen, ohne dass dieser von potentiellen Angreifern abgefangen oder erraten werden kann (siehe Schlüsselaustausch).

Asymmetrische Verfahren hingegen nutzen zwei unterschiedliche Schlüssel: einen öffentlichen Schlüssel, der ausschließlich zum vernicht jedoch zum entschlüsseln genutzt werden kann, und einen privaten Schlüssel, mit dem auch entschlüsselt werden kann. Bei dieser Konstellation kann der öffentliche Schlüssel ohne Probleme an beliebig viele Personen herausgegeben werden, da nur der Inhaber des privaten Schlüssels in der Lage ist, die mit dem öffentlichen Teil verschlossenen Daten zu entschlüsseln.

Stand der Technik bei symmetrischen Verschlüsselungsverfahren ist derzeit der Advanced Encryption Standard AES mit einer Schlüssellänge von 256bit, der nach heutigem Kenntnisstand mit verfügbarer Technik nicht „geknackt“ werden kann.

Schlüsselaustausch

Zur Gewährleistung einer sicheren Verschlüsselung ist es wie beschrieben notwendig, dass beide Kommunikationspartner über einen gemeinsamen geheimen und für Dritte nicht vorhersehbaren Schlüssel verfügen. Stand der



Sicherer Schlüsselaustausch nach dem Diffie-Hellman-Verfahren

Technik in diesem Bereich ist das Diffie-Hellman-Schlüsselaustauschverfahren: Ziel dieses Verfahrens ist es, dass beiden Kommunikationspartner derselbe geheime Schlüssel bekannt ist, ohne dass dieser jemals übertragen wurde. Hierzu wird von beiden Partnern separat eine Zufallszahl erzeugt, um aus dieser Zahl nach einem bekannten Algorithmus einen öffentlichen Schlüssel zu erzeugen, der dem jeweils anderen Partner zur Verfügung gestellt wird. Aus diesem öffentlichen Teil des Gegenübers und der ursprünglichen eigenen Zufallszahl kann im Anschluss von beiden Seiten ein Schlüssel errechnet werden, der trotz unterschiedlicher ⇨

- Ausgangszahlen beider Teilnehmer identisch ist und dennoch nie übertragen wurde.

Zufälligkeit des Schlüssels

Wie bereits ausgeführt, benötigen beide Kommunikationspartner für eine sichere symmetrische Verschlüsselung einen gemeinsamen Schlüssel, der niemandem außer diesen beiden bekannt sein darf. Diese Voraussetzung wird durch das Schlüsselaustauschverfahren sichergestellt. Falls dieses jedoch auf nicht wirklich zufälligen „Zufallszahlen" beruht, wird einem Angreifer die Möglichkeit gegeben, den Schlüssel zu erraten.

Bei einer üblichen Schlüssellänge von 256bit sind 10^{77} (eine Zahl mit 77 Nullen) verschiedene Schlüssel möglich, wodurch ein wahlloses Durchprobieren aller möglichen Schlüssel auch für moderne Hochleistungscomputer in vertretbarer Zeit nicht möglich ist. Damit diese Überlegung von Erfolg gekrönt ist, muss allerdings sichergestellt sein, dass die Wahrscheinlichkeit des Auftretens für jeden Schlüssel gleich groß ist. Sollten jedoch keine guten Zufallszahlen für die Schlüsselgenerierung genutzt werden, kann es passieren, dass von den 10^{77} möglichen Schlüsseln weit weniger in Frage kommen: Wenn einem Angreifer dieser Sachverhalt bekannt ist, muss er nur die in Frage kommende – und weit geringere – Anzahl an Schlüsseln durchprobieren. Die Wahrscheinlichkeit, in absehbarer Zeit den richtigen Schlüssel zu finden, ist somit deutlich größer.

Der Autor

Markus Schräder hat seit über 10 Jahren als Freelancer im IT-Security-Bereich für verschiedene Unternehmen gearbeitet und ist nun Geschäftsführer und Gesellschafter von CryptoMagic.

Schutz vor Orakeln

Im alten Griechenland versuchte man unter Zuhilfenahme des Orakels von Delphi Zukunftsprognosen zweifelhafter Qualität zu generieren. Im Kontext der Computerkryptographie bezeichnet ein Orakel hingegen ein System, welches durch sein nach außen sichtbares Verhalten Rückschlüsse auf die innere Funktionsweise und Entscheidungsfindung zulässt. Die Gefahr eines kryptographischen Orakels ist somit, dass es einem Angreifer durch sein Verhalten Anhaltspunkte liefert, um das Erraten des Schlüssels zu erleichtern.

Ein populäres Beispiel hierfür ist das Kinderspiel „Ich sehe etwas, das du nicht siehst...": Hierbei sucht sich der Spielleiter – das Orakel – einen Gegenstand aus, der erraten werden muss. Obwohl dieser anschließend nur Ja/Nein-Fragen beantwortet, haben die Mitspieler durch geschicktes Nachfragen die Möglichkeit, den gesuchten Gegenstand zu erraten.

Um dies zu verhindern, werden Verfahren wie HMAC oder GCM genutzt, um Anfragen zu signieren und so nur vertrauenswürdigen Kommunikationspartnern Antworten zu senden. Alle unsignierten Anfragen bleiben unbeantwortet. Durch dieses Vorgehen erhalten potentielle Angreifer möglichst wenige Reaktionen des Systems und sind folglich auch nicht in der Lage, Rückschlüsse zu ziehen.

Fazit

Eine sichere und vertrauenswürdige Verschlüsselung findet nur statt, wenn alle fünf Pfeiler berücksichtigt werden. Bereits das Nichtberücksichtigen eines der fünf Prinzipien führt zu einer angreifbaren und damit nicht sicheren Verschlüsselung.

Die Einhaltung der Prinzipien wird in der Regel durch die Nutzung offener Standards sichergestellt: Durch das Peer-Review werden so potentielle Schutzlücken entdeckt und können geschlossen werden. □

Cyber Security bei Videoanlagen

Digitalisierung und Vernetzung verändern auch die Videosicherheitstechnik grundlegend: Klassische analoge Videokameras mit direkt zugeordneten Videoaufzeichnungsgeräten werden durch immer leistungsfähigere IP-Kameras ersetzt, die in einer komplexen IT-Infrastruktur betrieben werden. Damit wachsen auch die Herausforderungen für einen sicheren Betrieb dieser Anlagen.

Von Hardo Naumann, Accellence Technologies

Intuitiv rechnen die meisten Menschen, wenn sie sich über Sicherheit Gedanken machen, mit Angriffen von außen. So ist es folgerichtig, dass bei den üblichen Firewall-Einstellungen vor allem Verbindungen, die von außen (aus dem Internet) nach innen (in das private Netz) aufgebaut werden, strengen Regeln unterliegen. Der Aufbau von Verbindungen von innen nach außen wird dagegen nur wenig reglementiert, um den Zugriff der Anwender auf die verschiedenen weltweiten Internet-Anwendungen und Dienste nicht zu beeinträchtigen.

Unterschätztes Risiko „embedded Systeme“

PCs und Server werden als sicherheitsrelevante Technik bewusst wahrgenommen. Risiken, die von embedded Systemen wie etwa Produkten aus dem Smart-Home-Bereich, „intelligenten“ Lautsprechern, Alarmanlagen und auch Kameras ausgehen, werden dagegen häufig unterschätzt. Bei Entwicklung und Auswahl von embedded Systemen stehen meist Funktion und Preis im Vordergrund. Das hat zur Folge, dass die Datensicherheit oft vernachlässigt wird.

Viele embedded Systeme bauen bereits ab Werk automatisch Verbindungen zu externen Servern auf, etwa für Updates, Fernwartung oder zum Speichern von Daten in der Cloud. Diese Verbindungen unterlaufen die Firewall; der Anwender hat in der Regel keine Kontrolle darüber, welche Daten über diese Verbindungen transportiert werden. Bei manchen Geräten sind Hintertüren bekannt geworden, die versehentlich oder absichtlich eingebaut wurden. Mitunter werden Geräte auch gezielt von Geheimdiensten, Industriespionen oder der organisierten Kriminalität manipuliert.

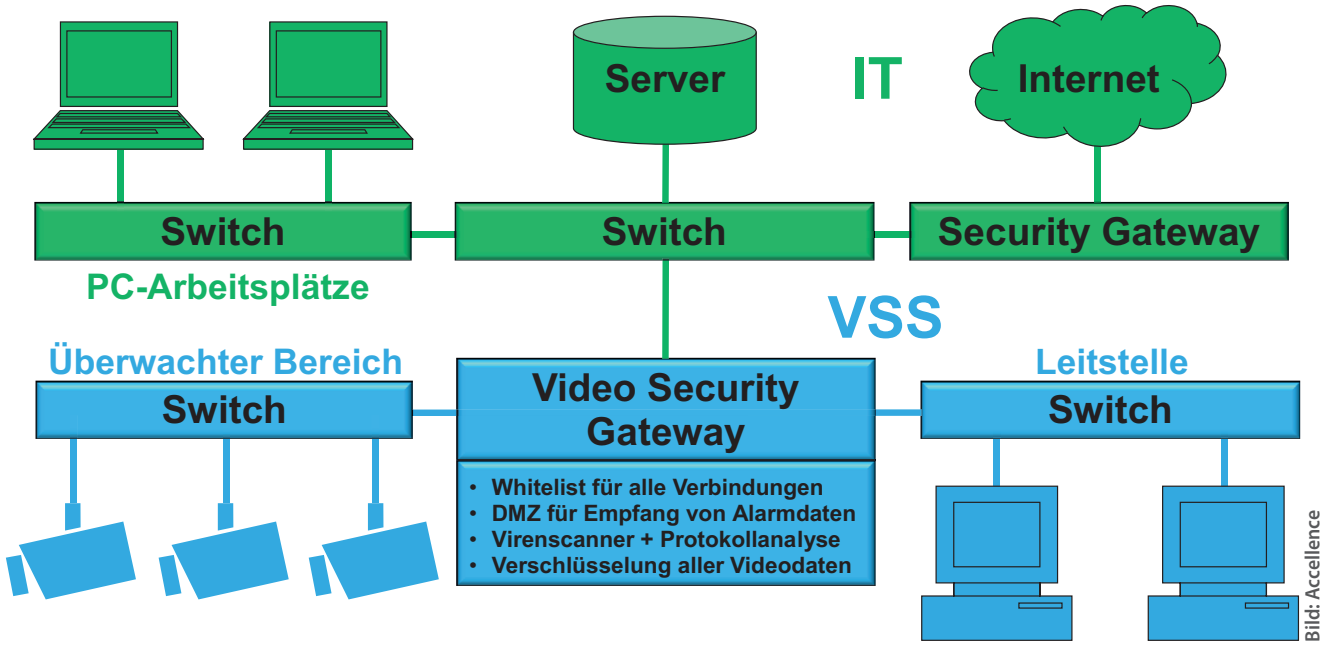
Dass diese Risiken nicht abstrakt und theoretisch sind, zeigt eine Vielzahl von Beispielen:

- Eine russische Hackergruppe hat im Zuge der Kampagne „Carbanak“ u.a. Überwachungskameras in Banken kompromittiert und konnte Millionenbeträge erbeuten.
- Die Schadsoftware „Mirai“ hat u.a. zahlreiche Überwachungskameras für einen DDoS-Angriff genutzt.
- Überwachungskameras des amerikanischen Herstellers „NetBotz“ waren jahrelang mit einer Hintertür in vielen Unternehmen und kritischen Bereichen eingesetzt.

Auch aus Gründen der Informationssicherheit und des Datenschutzes müssen Errichter und Betreiber von Videosicherheitssystemen sicherstellen, dass nur berechtigte Nutzer auf die Geräte und Daten zugreifen können.

Spezialfall „Video Sicherheits Systeme“

Für klassische Videoüberwachungsanlagen hat sich die Abkürzung „CCTV“ etabliert. Das CC ⇨



Kaskadierte Sicherheit: Ein Video Security Gateway sichert die Videoanlage gegenüber dem Unternehmensnetzwerk ab.

darin steht für „Closed Circuit". Damit ist gemeint, dass nur ein geschlossener Benutzerkreis auf diese Anlage und ihre Daten zugreifen kann. Mit der Umstellung auf IP ist grundsätzlich ein weltweiter Zugriff möglich. Deshalb muss durch geeignete technische Vorkehrungen dafür gesorgt werden, dass auch IP-basierte Videoanlagen wieder zu geschlossenen Systemen werden.

Während Anwender von ihrem IT-Endgerät (PC, Smartphone) weltweit uneingeschränkten Zugriff auf alle Anwendungen und Dienste wünschen, sollen bei Video Sicherheits Systemen (VSS) die Bilder einer begrenzten Anzahl Kameras nur auf einer wohldefinierten Auswahl von Monitoren dargestellt werden. VSS erlauben und erfordern deshalb engere Regeln als allgemeine IT-Systeme.

Die oberste Sicherheitsregel bei Video Sicherheits Systemen lautet: Das Netzwerk darf nur genau die explizit gewünschten Verbindungen zulassen; alle Verbindungsversuche zu anderen IP-Adressen müssen blockiert, protokolliert und gemeldet werden.

Lösungsalternativen

Das Risiko unerwünschter Verbindungen lässt sich durch geeignete technische Vorkehrungen vermeiden. Das ist vielleicht etwas aufwändiger und teurer, aber wenn die Sicherheit vernachlässigt wird, kann es auf lange Sicht sehr viel teurer werden.

Von Vorteil ist, bereits bei der Planung einer Videoanlage ein passendes Sicherheitskonzept zu wählen. Folgende Alternativen stehen zur Verfügung und können sich gegenseitig ergänzen:

1. Separates Netz für Video

Ein eigenes Netz für das VSS bietet die größte Sicherheit: Die physikalische Trennung von Leitungen kann von keiner Software überwunden werden. Höhere Kosten oder fehlende Kabeltrassen zwingen aber oft dazu, Video über vorhandene Leitungen zu transportieren. In diesen Fällen hilft

2. Virtual LAN – VLAN

Mit einem VLAN kann die vorhandene Verkabelung genutzt werden, um mehrere logisch

getrennte Netze zu realisieren. Dies erfordert durchgängig VLAN-fähige aktive Netzwerkkomponenten.

3. Virtual Private Network – VPN

VPN ist das Mittel der Wahl, wenn vertrauliche Daten über das Internet übertragen werden sollen. Alle Videodaten sind stets im LAN, VLAN und VPN zu halten, alle Verbindungen von und nach außerhalb dieses geschützten Bereichs sind zu sperren. Wichtig dabei: Netzwerkkopplung vermeiden! Geräte, die an mehrere Netze angeschlossen sind, können ungewollt Verbindungen zwischen diesen Netzen herstellen. Alle Geräte dürfen deshalb nur an ein Netz angeschlossen werden. Sind weitere Kommunikationsbeziehungen nötig, so sollten diese nur realisiert werden über ein

4. Video Security Gateway

Ein „Video Security Gateway" überwacht alle ein- und ausgehenden Verbindungen und kombiniert dabei verschiedene Sicherheitsmaßnahmen, die speziell auf die Belange der Videosicherheitstechnik im jeweiligen Anwendungsfall abgestimmt werden:

Die Firewall lässt nur die explizit gewünschten Verbindungen zu. Der Router stellt nach vorgegebenen Regeln Verbindungen her. Mittels Network Address Translation (NAT) werden dabei die IP-Adressen des internen Netzes vor der Außenwelt verborgen. Eine DMZ kann bei Bedarf eine Pufferzone zwischen äußerem und innerem Netz bilden. Die Protokollanalyse erkennt verdächtigen Datenverkehr. Ein Virenscanner prüft alle eintreffenden Daten auf Schadcode. Auch wenn die Videoübertragung z.B. nur für TCP/IPv4 ausgelegt ist, könnte Schadsoftware auch IPv6, ICMP, DNS oder den UDP-Protokollstack nutzen. Schadsoftware zweckentfremdet gern Standardports und unverdächtige Protokolle und wird nur spontan aktiv. Deshalb muss das Security Gateway dauerhaft alle Verbindungen überwachen, nicht nur die vom VSS genutzten.

5. Verschlüsselung

Eine durchgängige „Ende-zu-Ende-Verschlüsselung" stellt sicher, dass niemand unbefugt auf die Videodaten zugreifen kann. Die Verschlüsselung kann alternativ auch im Video Security Gateway erfolgen. Dies ist insbesondere dann geboten, wenn Videodaten z.B. in der „Cloud" gespeichert werden sollen. Entscheidend ist dabei: Wer besitzt den Schlüssel?

Weiterführende Informationen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die erste Adresse für IT-Sicherheit in Deutschland. Es stellt kostenlos Dokumente mit Empfehlungen u.a. zum Sicherheitsmanagement und IT-Grundschutz zum Download bereit. Aktuell sind dort neue Bausteine zu embedded Systemen (IoT) und IP-Kameras erschienen.

Im BHE Bundesverband Sicherheitstechnik e.V. arbeiten Hersteller und Errichter von Sicherheitssystemen zusammen. Der BHE veranstaltet Seminare und Kongresse, in Fachausschüssen werden Informationspapiere erarbeitet.

Holen Sie sich fachkundigen Rat, wenn Sie eine Videoanlage planen oder betreiben. Firmen wie Accellence Technologies in Hannover bieten umfassende Beratung und entwickeln spezielle Lösungen für die Videosicherheit. □

Der Autor

Dipl.-Ing. Hardo Naumann
ist General Manager für Alarm Receiving Solutions bei der Accellence Technologies GmbH und Mitglied im Fachausschuss „Video" des BHE.

Wie sicher sind Ihre mobilen Geräte?

Bild: certgate

Die moderne Arbeitswelt unterliegt einem stetigen Wandel. Morgens im Auto, mittags im Büro, nachmittags beim Geschäftspartner oder Kunden und abends noch ein paar schnelle Aufgaben im Home (Office) erledigt. Durch die zunehmende Digitalisierung ist Mobilität heute oft keine Option mehr, sondern Voraussetzung für erfolgreiche Unternehmen und Geschäftsmodelle.

Von Jan C. Wendenburg, certgate

Diese Mobilität ermöglicht verbesserte Produktivität und Auslastung der Ressourcen – aber auch erhöhte Flexibilität für die Mitarbeiter. Home Office, eine Videokonferenz von unterwegs, eine E-Mail aus dem Urlaub sind praktisch für alle Beteiligten. Dieser mobile Zugriff auf Daten – von überall und egal welcher Art – erfordert aber auch entsprechende mobile Sicherheit. Überall, jederzeit, für alle Daten.

Neue Herausforderungen an die IT

Neben dem Faktor Mensch stellen heute mobile Endgeräte das größte Sicherheitsrisiko im Netzwerk eines Unternehmens dar. Die Umsetzung der Sicherheit der Informationstechnik (und oft auch deren Überwachung) ist in der Regel Verantwortung der IT-Abteilung. Neben üblichen zentralen Systemen wie Firewalls, IDS etc. und für Management, Steuerung und Überwachung mobiler Geräte (MDM, MAM, EMM, etc.) ist gerade auch die langfristig berechenbare Sicherheit der Endgeräte selbst, bzw. der Apps und Daten, entscheidend.

Da sich die mobilen Geräte im Wesentlichen nur noch auf drei Plattformen (iOS, Android und für Laptops Windows) beschränken, sind auch alle drei Plattformen häufig in Unternehmen und Organisationen anzutreffen. Windows-Systeme haben eine lange Historie und breite Auswahl in der Unterstützung von „Enterprise-Level“ Management, Verschlüsselungs- und Authentifizierungslösungen. iOS und Android stecken teilweise bei der mobilen Sicherheit noch in den Kinderschuhen, haben aber auch schon einiges in den letzten Jahren nachgeholt und verbessert.

Neue Konzepte, wie Bring Your Own Device (BYOD) machen es für die IT-Sicherheit auch nicht einfacher, da nun die (vertraulichen) Daten auf „fremden“ Geräten gespeichert werden. D.h. eine zentral berechenbare, eindeutige Gerätesicherheit ist nicht mehr überall nachvollziehbar.

Zusätzlich sind die Anforderungen an eine einfache Bedienung von Hardware und Software durch „Consumer“-Endgeräte wie Smartphones etc. exponentiell gestiegen. Eigentlich hat da mobile Sicherheit keinen Platz – und wird als separate Anwendung oder als zusätzlich erforderliche, meist komplexe Eingaben von vielen

Anwendern abgelehnt. Mobile Sicherheit soll und muss im Hintergrund arbeiten. Wie eine Heizung im Keller: Wenn sie funktioniert, merkt es keiner – erst wenn etwas ausfällt, darf es Alarm geben.
Also einfacher, schneller, individueller und mobiler? Eine starke Herausforderung für jede IT.

Mobile Sicherheit durch Verschlüsselung

Mobile Geräte verfügen heute über Speicherkapazitäten von 64, 128 oder 512 GB. Das ist mehr als vor wenigen Jahren die zentralen Daten-Server der meisten Unternehmen hatten. So werden auf diesen Geräten heute alle Arten von vertraulichen Unternehmensdaten gespeichert: E-Mails, Präsentationen, Excel-Daten, CRM, ERP und Personal-Informationen; auch branchenspezifische, wie Gesundheits-/Patientendaten, Konstruktionszeichnungen, Forschungsergebnisse. Eine klare, nachvollziehbare Unterscheidung von vertraulichen Daten und nicht-vertraulichen Daten ist dabei in der Regel nicht mehr möglich.
Mobile Geräte haben naturgemäß ein erhöhtes Risiko des Verlustes und von unautorisiertem Zugriff. Daher sollte ein nachhaltiger Schutz dieser wichtigen Daten immer über langfristig berechenbare und – sehr wichtig – Endgeräte-unabhängige 2-Faktor-Sicherheitsmechanismen erfolgen.
Wenn Daten und Zugriff nach modernen Methoden und Standards verschlüsselt werden, ist in der Regel ein ausreichender Schutz gegeben. Jede Verschlüsselung benötigt die Schlüssel zum ver- und entschlüsseln. Diese Schlüssel müssen langfristig berechenbar und sicher sein, d.h. unabhängig von der eingesetzten Endgeräte-Technologie gespeichert sein. Die dazu passende 2-Faktor-Lösung – Chip-basierte Smartcards – gibt es schon seit vielen Jahren, hat sich aber aufgrund von erhöhter Komplexität und geringer Bedienungsfreundlichkeit nur wenig verbreitet. Gerade mobile Endgeräte und Smartcards passten bisher kaum zusammen.

Neue Produkte ermöglichen sichere Mobilität mit zertifizierter Sicherheit

In den letzten Monaten sind hier nun neue Konzepte und marktreife Produkte zu erkennen. So können jetzt Smartcards einfach in Schlüsselanhänger oder „Badges“, d.h. Sichtausweishüllen, eingesteckt und drahtlos via Bluetooth mit Endgeräten verbunden werden. Der Endbenutzer kann erstmals so mobil arbeiten wie bisher, jedoch geschützt durch unabhängig zertifizierte Schlüsselspeicher (Common Criteria, EAL 5). Die Sicherheit dieser Schlüssel ist unabhängig von den Endgeräten und damit auch geeignet für heterogene Plattformen (Windows, Android, iOS) und BYOD-Umgebungen. Ebenfalls ist eine mobile Geräte- und Plattform-übergreifende, sichere 2-Faktor-Authentifizierung gewährleistet und darüber hinaus sind Zusatzfunktionen, wie Zugang oder Bezahlen per NFC, ebenfalls möglich.
Namhafte, globale Unternehmen, wie z.B. im Automotive-Bereich, haben bereits die Vorteile dieser neuen Technologie erkannt und setzen diese zum Schutz ihrer mobilen Mitarbeiter und Infrastruktur produktiv ein. □

Der Autor

Jan C. Wendenburg ist CEO der certgate GmbH in Nürnberg, hat diverse IT-Unternehmen erfolgreich gegründet und verfügt über langjährige Management-Erfahrung bei IBM, im Venture Capital-Bereich und im globalen IT-Security-Markt. certgate konnte so in den letzten Monaten vom lokalen Hardware-Anbieter zu einem internationalen Hardware & Software-Anbieter mit zusätzlichen Standorten in Hannover und Düsseldorf expandieren.

Abschied vom ISDN: So gelingt der sichere Umstieg auf VoIP

Bis Ende 2018 möchte die Telekom alle analogen und ISDN-Anschlüsse auf IP-basierte Netze migrieren. Mit dieser Überführung in All-IP-Netze reihen sich Sprachdaten dann erstmals flächendeckend in die Riege IP-basierter Anwendungen ein.

Von Dr. Martin Krebs, Lancom Systems

Dies bringt vielschichtige neue Anforderungen an die Netzwerkinfrastruktur mit sich. Neben einem VoIP-fähigen Router, der den Annex-J-Standard unterstützt, und dem Vorhandensein geeigneter Quality-of-Service-Mechanismen, muss nicht zuletzt die Netzwerksicherheit auf den Prüfstand gestellt werden.

Grundsätzlich spielen Firewalls eine zentrale Rolle, wenn es um die Absicherung von IP-Netzwerken geht. Sie schützen das LAN vor unbefugtem Zugriff, indem sie den durchlaufenden Verkehr überwachen und regelbasierend entscheiden, ob bestimmte Datenpakete durchgelassen werden.

Bei SIP-basierten Sprachpaketen (Voice over IP) gelangen Firewalls jedoch an ihre Grenzen. Der Grund liegt darin, dass SIP-Pakete die benutzten Ports dynamisch aushandeln und in der Payload übermitteln. Einfach alle Ports für VoIP und Multimedia-Anwendungen „per se“ zu öffnen, wäre keine gute Idee. Sonst böten alle VoIP-Endgeräte als mit der Außenwelt verbundene „Mini-Rechner“ Zugang zum Firmennetz. Oder sie könnten – entsprechend manipuliert – leicht zum Abhören oder Mitschneiden von Gesprächen, beispielsweise durch ein von außen gesteuertes Aktivieren der Mikrofone, missbraucht werden. Um dieser potenziellen Schwachstelle entgegenzuwirken, ist eine saubere Trennung des (unsicheren) externen Netzes vom (sicheren) internen Netz erforderlich. Hierdurch kommt eine für viele Netzwerkadministratoren neue Komponente ins Spiel: der Session Border Controller.

Funktionsweise eines Session Border Controllers

Ein „Session Border Controller“ (SBC) kontrolliert den Auf- und Abbau sogenannter Sitzungen („Sessions“) an der Netzwerkgrenze („Border“). Im Gegensatz zu einer Firewall ist ein SBC in der Lage, an der Netzwerkgrenze Echtzeit-SIP-Kommunikation im Bereich der Signalisierungsdaten (Control Plane) und der Sprach- beziehungsweise Mediadaten (Data Plane) zu untersuchen. Er steuert den Aufbau, die Durchführung und den Abbau von Telefonaten und die dazugehörigen Datenströme bezüglich Signalisierung und Mediendaten wie Sprache oder Video.

Als Proxy für SIP-Kommunikation terminiert ein SBC zunächst jede Session, beispielsweise einen extern eingehenden Anruf, und setzt anschließend eine neue Session für das interne Gespräch auf. Bei diesem Vorgang werden Signalisierungsdaten und Media Streams untersucht, validiert und gegebenenfalls transformiert. Dabei kommen die Vorteile eines SBCs in den

Bild: Lancom Systems

Funktionsweise eines Session Border Controllers

Bereichen Sicherheit und Qualität zum Tragen. Im SBC eingehende und ausgehende Sessions werden terminiert. Nur bekannte und unterstützte Steuerungsbefehle werden weitergeleitet. Dabei bietet der SBC als Applikations-Firewall Zugangsschutz für Sprache, Video und Multimedia. Er überwacht erlaubte Sessions und versteckt ihren topologischen Ursprung, wie beispielsweise interne IP-Adressen von Servern und Telefonen. Darüber hinaus schützt der SBC die Vertraulichkeit von Echtzeit-Sprachdaten gegen Abhören, Mitschneiden und Man-in-the-Middle-Attacken durch die optionale Verschlüsselung per AES (Secure Real-Time Transport Protocol, SRTP). Wenn Telefone im LAN, am ISDN oder am Analog-Port einer TK-Anlage keine verschlüsselte Sprachtelefonie können, kann der SBC die Telefonie zum Provider dennoch verschlüsseln und wieder entschlüsseln. So können VoIP-Daten selbst dann verschlüsselt werden, wenn es die Telefone nicht können. Voraussetzung hierfür ist jedoch, dass die Gegenstelle – beispielsweise ein SBC auf Providerseite – die so verschlüsselten Pakete wieder entschlüsseln kann. Ebenso werden ausgehende Signalisierungsdaten über TLS verschlüsselt (Session Initiation Protocol Secure, SIPS) und bei Eingang entsprechend entschlüsselt.

Ende-zu Ende-Verschlüsselung

Auf diese Weise wird allerdings nur die Verbindung zwischen Anrufer und dem Provider verschlüsselt. Um eine durchgängige Verschlüsselung zwischen beiden Teilnehmern zu erreichen, sollten sie idealerweise beim gleichen Provider registriert sein. Dies gewährleistet aber nicht eine durchgängige Ende-zu-Ende-Verschlüsselung. Der Grund ist politisch: In den meisten Ländern muss der SBC des Providers die Daten entschlüsseln können, um Sicherheitsbehörden gegebenenfalls Zugriff auf den durchgeleiteten Datenverkehr geben zu können. Eine durchgängige Verschlüsselung lässt sich somit nur durch eine direkte, verschlüsselte Verbindung zwischen den Session Border Controllern der Gesprächsteilnehmer, beispielsweise mit einem VPN-Tunnel, erreichen. Voraussetzung ist allerdings eine garantierte Backdoor-Freiheit der verwendeten Produkte. Spezielle Software auf mobilen Geräten bietet ebenfalls Möglichkeiten zur durchgängigen Ende-zu-Ende-Verschlüsselung. □

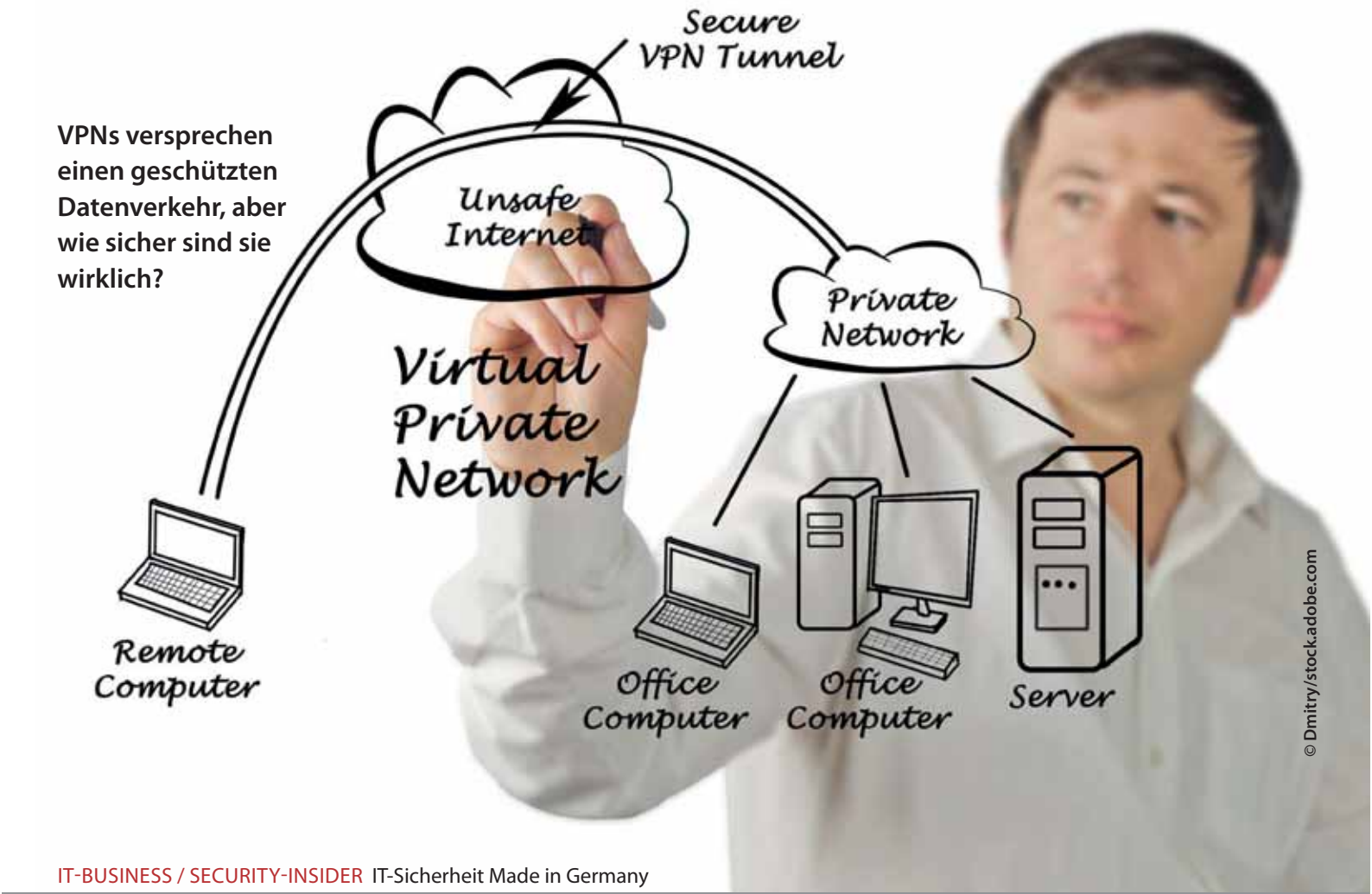
Der Autor

Dr. Martin Krebs hat an der RWTH-Aachen Informatik studiert und dort auch promoviert. Bei Lancom Systems ist er als Leiter Produktmanagement verantwortlich für das Produktportfolio aus Hardware und Software.

Virtual Private Network? – Schwachstellen, Angriffspunkte und Schutzmaßnahmen

Durch die fortschreitende Digitalisierung wird das Arbeiten zunehmend flexibler. Mobile Endgeräte ermöglichen es, jederzeit erreichbar zu sein und der Arbeit ohne Einschränkungen nachzugehen. Die Anzahl und Verwendung öffentlicher Netzwerke, wie z.B. in Cafés und Zügen, steigt. Um nicht nur effizient, sondern auch sicher von überall aus arbeiten zu können, scheint VPN die perfekte Lösung zu sein. Doch wie sicher ist der Datenverkehr über Virtual Private Networks wirklich?

Dario Engelmayer, Sama Partners



VPNs versprechen einen geschützten Datenverkehr, aber wie sicher sind sie wirklich?

© Dmitry/stock.adobe.com

Tägliche Szenarien und deren Gefahren

Soviel vorweg: Das Arbeiten in öffentlichen Netzen kann, selbst unter Verwendung von VPN, unsicher sein. Denn Angreifer können dem Netzwerk beitreten, ohne dieses vorher attackieren bzw. kompromittieren zu müssen. Falsche Konfigurationen sowie die Verwendung von „Split Tunneling“ erhöhen das Risiko eines Datendiebstahls.

Private Netzwerke werden meist weder von deren Besitzern überwacht, noch durch Sicherheitsmaßnahmen wie Firewalls, IDS, etc. auf dem Level eines Firmennetzwerks abgesichert. Angreifer können daher leicht in das Netz eindringen und deren Clients ins Visier nehmen.

Ist der Client erst kompromittiert, vereinfacht sich das Eindringen in ein Firmennetzwerk deutlich. Denn durch die VPN-Verbindung können Angreifer einige Sicherheitsmaßnahmen schon mit weitaus geringerem Aufwand umgehen, da sie (virtuell) Teil des internen Netzes sind.

Welche Angriffspunkte bietet VPN und welche Schutzmaßnahmen gibt es?

Vorkommnisse aus der Vergangenheit zeigen, welche Folgen schlecht konfigurierte VPNs und fehlende Sicherheitsmechanismen haben können. So musste bspw. das in Tennessee ansässige Unternehmen Community Health Systems enorme Schäden durch den „Heartbleed Bug“ (CVE-2014-0160) hinnehmen. Den Angreifern war es 2014 gelungen, die VPN-Login-Daten von einem Test-Server mithilfe von „Buffer Over-Read“ auszulesen. Mit diesen Daten konnten sie sich anschließend in das produktive System einloggen und 4,5 Millionen Patientendaten stehlen.

Dieser Vorfall wäre durch die Verwendung verschiedener Logins für Test- und Produktiv-Systeme vermeidbar gewesen. Außerdem hätte durch das Einsetzen einer Zwei-Faktor-Authentifizierung eine weitere Sicherheitsebene hinzugefügt und damit das Risiko verringert werden können. Grundsätzlich gilt ferner: Ein Testsystem sollte nach Möglichkeit nie über das Internet zu erreichen sein. Denn auch das stellt eine Gefahr dar.

Clientless oder Portal VPNs

Clientless oder Portal VPNs können viele Szenarien, wie zum Beispiel die Verwendung verschiedener Betriebssysteme, vereinfachen. Jedoch sollten die damit verbundenen Risiken betrachtet und Konfigurationen von geschultem Personal durchgeführt werden.

Unter der Kennzeichnung „CVE-2014-3393“ führt die CVE-Datenbank (Common Vulnerabilities and Exposures) eine Verwundbarkeit des Cisco Clientless VPNs. Diese entstand durch ein Feature, welches den Unternehmen das Anpassen des Anmeldeportals an Corporate Styles gestattete. Die Funktion gewährte die Installation von Drittanbieterprodukten und das Integrieren eigener Skripte, was es den Angreifern ermöglichte, Cross-Site-Scripts zu implementieren und Anmeldedaten der Benutzer mitzuschneiden.

Laut Volexity wäre die Verwendung einer Zwei-Faktor-Authentifizierung als Sicherheitsmaßnahme in diesem Fall nicht ausreichend gewesen, da auch Session Cookies extrahiert werden konnten. Cisco reagierte schnell auf die Veröffentlichung der Sicherheitslücke und schloss sie mit einem Update. Doch ließen sich einige Unternehmen viel Zeit mit der Aktualisierung und „servierten sich somit selbst auf dem Präsentierteller“ – spätestens nachdem der Vulnerability Scanner Nessus mit dem Plug-In „ID 78240“ auf die Verwundbarkeit prüfen konnte. Administratoren sollten ihre Applikationen also regelmäßig auf Aktualisierungen prüfen und Sicherheitslücken nach Bekanntgabe schnellstmöglich schließen.

- Bei Verwendung des Portal VPNs entsteht ein zusätzliches Risiko, da nur der Verkehr des Browsers bzw. des darin genutzten Portals durch den Tunnel geleitet wird. Andere Applikationen verbinden sich weiterhin, gegebenenfalls unverschlüsselt, mit dem Internet. In diesem Zusammenhang gilt es darauf hinzuweisen, dass VPN Services aus dem Internet oftmals nicht zu empfehlen sind. Häufig versprechen diese zwar absolute Sicherheit und Anonymität, durch das Loggen und langfristige Speichern der Daten kann dies aber nicht sichergestellt werden.

Split Tunneling, SSL VPNs und Social Engineering

Split Tunneling wird gerne genutzt, um die Performance von VPNs zu steigern und Peripherien, wie einen Netzwerkdrucker, weiterhin zu verwenden. Die für das Unternehmen relevanten Daten werden verschlüsselt durch den Tunnel in das Firmennetzwerk geleitet, der Rest wird unverschlüsselt in das Internet übertragen. Durch die direkte Anbindung an das Internet ist der Client aber einem höheren Risiko ausgesetzt, kompromittiert zu werden, und kann als Gateway, der in das Firmennetzwerk führt, fungieren.

Bei der Verwendung von SSL VPNs wird das Zertifikat auf dem Computer bzw. unter dem Benutzerkonto gespeichert. Wird der PC nun entwendet oder kompromittiert, kann das Zertifikat kopiert und von Unberechtigten benutzt werden. Möglich ist auch der Angriff auf eine Zertifizierungsstelle und das Ausstellen vermeintlich „sicherer" Zertifikate, wie es 2011 bei Comodo der Fall war.

Auch das Social Engineering kann ein Angriffsweg sein. Um die Risiken in diesem Bereich zu vermeiden, sollte jedes Unternehmen Awareness-Schulungen und andere Awareness-Maßnahmen für die Mitarbeiter, gemäß ISO 27001, durchführen. Schulungen, die auch private Interessen einbeziehen, vermitteln den Inhalt oftmals besser. Denn: Wer zuhause sensibel reagiert, wird dies unbewusst auch im Arbeitsalltag tun.

Fazit

Wer ein flexibles Arbeitsumfeld wünscht, sollte bedenken, dass auch hinter VPN nur ein Stück Software steckt. Folglich entstehen hier nicht weniger Sicherheitslücken als bei jeder anderen Applikation. Wie so oft muss bei der Wahl der Variante das richtige Maß zwischen Sicherheit und Benutzerfreundlichkeit gefunden werden. Das Verwenden einer Zwei-Faktor-Authentifizierung ist in einigen Fällen vielleicht nicht ausreichend, sollte jedoch als zusätzliche Sicherheitsebene in Betracht gezogen werden.

Außerdem sind regelmäßige Awareness Schulungen für Mitarbeiter und der Einsatz von Medien, wie bspw. Plakate, zur Erinnerung der wesentlichen Inhalte, sehr zu empfehlen. Eine zusätzliche fachspezifische Schulung der Administratoren, hinsichtlich Risiken und Sicherheitsmaßnahmen, ist darüber hinaus unerlässlich.

Vor allem aber sollten Unternehmen und deren IT-Fachkräfte nach Bekanntgabe von Sicherheitslücken sowie deren Patches schnell reagieren und diese schließen bzw. einspielen.

Auch die regelmäßige Kontrolle der VPN Logs auf Unstimmigkeiten ist eine gute Methode, um eventuelle Einbrüche aufzuspüren und weitere Schäden zu verhindern. □

Der Autor

Dario Engelmayer ist Security Consultant beim IT-Beratungshaus Sama Partners in Mannheim und Referent auf der jährlich stattfindenden Cybersecurity Conference.

Wenn Passwörter nicht mehr greifen – Multi-Faktor-Authentifizierung schützt digitale Identitäten

Kein Tag vergeht ohne Meldungen über gehackte Datenbanken, gestohlene Passwörter oder manipulierte digitale Identitäten. Allein die Website haveibeenpwned.com hat mittlerweile über 4,7 Milliarden gehackte Accounts registriert. Es ist davon auszugehen, dass die Dunkelziffer der Datendiebstähle noch weit darüber liegt. Bis die Unternehmen die Hacks bemerken, vergehen durchschnittlich mehr als vier Monate, bei Behörden bis zu einem Jahr.

Von Dr. Amir Alsbih, Keyldentity

Je länger die Angreifer unentdeckt bleiben, desto mehr Daten können sie erbeuten und missbrauchen. Denn viele Nutzer verwenden ihre Passwörter mehrfach für unterschiedliche Portale – von Datenbanken im Unternehmen über den privaten Google- oder Apple-Account, Social-Media-Profile bei Facebook oder Twitter bis hin zu Amazon oder eBay. Sind die Täter erst einmal in diese Sphären vorgedrungen, sind Schäden an der digitalen Identität Tür und Tor geöffnet.

Sie können zum Beispiel die Verknüpfung zwischen E-Mail-Account und eBay-Konto aufheben, so dass der Kontoinhaber nicht mehr benachrichtigt wird, wenn ein Krimineller in seinem Namen Produkte auf eBay kauft und verkauft. Angreifer können auch Hintertüren (Backdoors) in das Netzwerk integrieren oder andere Systeme so manipulieren, dass die hinterlegten Daten überhaupt nicht mehr genutzt werden können.

Wenn sie mehrere Monate für diese Übergriffe Zeit haben, entstehen Schäden, die nicht mehr durch Backups oder Datenwiederherstellungen ausgebessert werden können.

Passwörter in über 80 Prozent der Fälle Ursache für Hacks

Die Liste der Beispiele für den Missbrauch digitaler Identitäten lässt sich beliebig fortsetzen. Doch sie haben eines gemeinsam: Der Schwachpunkt ist immer das Passwort. Waren Passwörter 2016 noch die Ursache für etwa 60 Prozent aller Hacks, sind es heute schon über 80 Prozent. Trotz des großen Risikos sind Passwörter noch immer die meistgenutzte Authenti- ⇨

fizierungslösung. Anstatt bereits verfügbare sichere Alternativen zu implementieren, werden Passwörter komplexer gemacht – mit zehn Zeichen sowie Klein- und Großbuchstaben, Ziffern und Sonderzeichen als Mindestanforderung. Da sich diese Passwörter kein Nutzer mehr merken kann – insbesondere wenn er mehrere Zugangsdaten für unterschiedliche Webportale verwendet – greifen viele zur Papiernotiz oder zu Mustern.

Was nur die wenigsten Nutzer wissen oder wahrhaben wollen: Diese Muster machen es Kriminellen viel leichter, die Passwörter systematisch zu erraten. Sie müssen deutlich weniger Zahlen- und Buchstabenkombinationen durchprobieren und kommen dadurch schneller an ihr Ziel. Nicht unterschätzt werden sollte dabei auch das „Targeted Password Guessing“: Auf Basis soziodemographischer Daten wie Name, Geburtstag oder Telefonnummer, die oftmals über soziale Netzwerke frei zugänglich sind, lassen sich Passwörter erschreckend einfach ableiten.

Einfach und sicher zugleich: Multi-Faktor-Authentifizierung

Die beschriebenen Szenarien machen eines ganz deutlich: Es ist an der Zeit, digitale Identitäten besser zu schützen – vor allem vor dem Hintergrund von Sicherheitsvorgaben wie der EU-Datenschutz-Grundverordnung (EU-DSGVO), der EU-Zahlungsdienste-Richtlinie PSD2 oder dem IT-Sicherheitsgesetz. Dafür müssen Logins und Transaktionen umfassend sicherer gestaltet werden. Die Alternative zu Passwörtern heißt hierbei Multi-Faktor-Authentifizierung (MFA). Auch der Bundesverband IT-Sicherheit e.V. (TeleTrusT) empfiehlt die Technologie in einer aktuellen Handreichung zum IT-Sicherheitsgesetz. Ebenso schützen mittlerweile auch viele internationale Player wie Google, Apple oder Facebook die digitalen Identitäten ihrer Kunden mit diesen Lösungen.

Bild: KeyIdentity

Beim Einsatz der Multi-Faktor-Authentifizierung können Unternehmen und Behörden aus einer großen Bandbreite an Token-Typen wählen – je nach Sicherheitslevel des Nutzers.

Bei der Multi-Faktor-Authentifizierung werden mindestens zwei Berechtigungsnachweise (Faktoren) miteinander kombiniert. Meldet sich der Nutzer beispielsweise an einem Webportal an, erhält er einen Einmal-Code auf sein Smartphone oder generiert diesen über ein sogenanntes Hardware-Token. Nur wenn er diese Daten eingibt, wird das Login oder die Transaktion bestätigt. Diese Lösung ist deutlich sicherer als

die Eingabe von Passwörtern, da ein Angreifer zunächst an den zweiten Faktor gelangen muss, welcher in der Regel mit einem physischen Gegenstand verknüpft ist. Darüber hinaus müssen sich Nutzer nicht mehr viele verschiedene Passwörter merken und können sich auf ihre eigentliche Tätigkeit konzentrieren.

Große Auswahl an MFA-Token

Beim Einsatz der Multi-Faktor-Authentifizierung können Unternehmen und Behörden aus einer großen Bandbreite an Token-Typen wählen – je nach Sicherheitslevel des Nutzers. Die Möglichkeiten reichen dabei von vergleichsweise weit verbreiteten SMS-Token, welche die Identität über die eigene Telefonnummer bestätigen, über Software-Token sowie Hardware-Token in der Größe eines Schlüsselanhängers bis hin zu den zukunftweisenden QR- und Push-Token.

Letztere Token-Typen zeichnen sich insbesondere durch die einzigartige Kombination höchster Sicherheit und Usability aus. Sie ermöglichen zudem die Absicherung von Transaktionen durch die Verwendung kryptographischer Methoden. Dabei wird Integrität gewährleistet und Nicht-Abstreitbarkeit realisiert.

Bei der Push-Authentifizierung wird beispielsweise eine Push-Benachrichtigung auf das Smartphone des Nutzers gesendet, sobald er sich einloggen oder eine Transaktion durchführen will. Er muss dann nur noch auf „OK“ oder „Nicht OK“ klicken.

Bei QR-Token scannt der Anwender einfach per Smartphone-Kamera den entsprechenden QR-Code ein – das funktioniert bei der KeyIdentity Open-Source-Lösung LinOTP sogar offline im Flugzeug oder in hochsicheren Umgebungen, in denen kein WLAN gestattet ist. Einfacher und schneller geht es kaum. Mit Hilfe dieser neuen Token-Typen lässt sich auch ein Mehraugenprinzip bei Transaktionen problemlos umsetzen. Dies kann zum Beispiel erforderlich sein, wenn im Unternehmen oder bei einer Investmentbank eine große Überweisung genehmigt werden muss.

Handeln ist gefragt

Laut BSI ist jedes zweite Unternehmen von Cyberangriffen betroffen. Vor dem Hintergrund dieser Bedrohungen müssen die Verantwortlichen endlich aktiv werden. Tun sie es nicht, handeln CEOs, CIOs oder CISOs heute grob fahrlässig – denn es ist nur eine Frage der Zeit, bis auch sie von Datendiebstahl, versehentlichen Fehlern der Nutzer oder einem ausgefeilten Cyberangriff durch Kriminelle betroffen sind. Wenn sich Unternehmen und Behörden für eine MFA-Lösung entscheiden, sollten bei der Auswahl vor allem eine schnelle Integration in bestehende IT-Umgebungen im Fokus stehen sowie eine hohe Skalierbarkeit, um auch für künftige Anforderungen gerüstet zu sein. Die MFA-Lösung sollte auch smarte Features mitbringen, die dazu beitragen, die operationalen Kosten sowie den Aufwand für die IT im Unternehmen zu senken. Außerdem sollten Usability und Sicherheit stets berücksichtigt werden. Denn nur wenn die Tools auch genutzt werden, können sie höchste Security gewährleisten. □

Der Autor

Dr. Amir Alsbih leitet als Chief Operating Officer (COO) das weltweite operative Geschäft der KeyIdentity GmbH. In dieser Funktion zeichnet er für die globalen Geschäftsprozesse des führenden Anbieters von hoch skalierbaren und schnell einsetzbaren Multi-Faktor-Authentifizierungslösungen (MFA) mit Open-Source-Kern verantwortlich.

Der gordische Knoten – Datenschutz und EDV

Die Art und Weise wie personenbezogene Daten verarbeitet werden hat sich in den letzten Jahrzehnten beständig verändert und erweitert. In den letzten Jahren wurde bereits sehr viel von Papier in Bits und Bytes umgewandelt. Die Digitalisierung schreitet also schon seit Jahren voran, ganz ohne Gesetzesinitiativen und Maßnahmenpakete oder haben Sie noch eine Schreibmaschine, um einen Arbeitsvertrag zu verfassen?

Von Peter Liebing und Alexander Schuschies, digitronic computersysteme

Entstehungsgeschichte

Artikel 12 der Charta der Menschenrechte der Vereinten Nationen beschreibt das Recht auf Privatsphäre – und somit auch das Briefgeheimnis. In der Charta der Grundrechte der Europäischen Union wurde das Recht auf Privatsphäre in Artikel 7 um ein Recht auf den Schutz personenbezogener Daten – in Artikel 8 – erweitert.
Die Praxis hat den Gesetzgeber jedoch längst überholt und überrollt. Man macht, was bequem und praktisch ist. Dabei hat man vergessen, dass der Arbeitsvertrag früher im Aktenschrank verschlossen lag, heute liegt er auf dem Fileserver oder in der Cloud. Aber wer diesen dort lesen kann, darüber wollte man sich besser keine Gedanken machen. Bei den „Kronjuwelen", Prototypen-Daten, Konstruktionszeichnungen und Partnerverträgen hat man inzwischen gemerkt, wie existenzbedrohend es sein kann, wenn man den Zugriff nicht mehr selbst steuern kann. Bei den Daten der Mitarbeiter und Kunden hat man lange geschlafen.
Deshalb wurde nun die EU-Datenschutz-Grundverordnung novelliert, um Artikel 8 zu spezifizieren und auf die neuen Gegebenheiten anzupassen.

Der Streitwagen des Gordios

Die Anforderungen an die Vertraulichkeit sensibler Daten steigen rasant, auch im Zusammenhang mit rechtlichen Vorgaben. Denken wir nur an die Umsetzung technischer Anforderungen nach VDA ISA für den Zugang zu Datennetzen von Automobilherstellern (z. B. bei der Prüfung ihrer Informationssicherheit im Rahmen von TISAX) oder an die besagte Europäische Datenschutz-Grundverordnung. Nicht zu vergessen, die Realisierung der technischen Anforderungen im Rahmen einer ISO 27001-Zertifizierung und zu guter Letzt an die Absicherung kritischer Informationsinfrastrukturen KRITIS

nach dem aktuellen Stand der Technik, z. B. in den Sektoren Energie, Gesundheit, Banken und Versicherungen.

Der gordische Knoten

Stehen sich damit also zwei Entwicklungen konträr gegenüber? Der Schutz der personenbezogenen Daten meiner Mitarbeiter und Kunden gegen meine Bequemlichkeit der Datenverarbeitung? Die Paranoia meines Datenschutzbeauftragten, dass selbst Daten eines gerade in der Bearbeitung befindlichen Word-Dokuments ausgelesen werden? Lässt sich der gordische Knoten lösen?

Zunächst sollte geklärt werden, was personenbezogene Daten sind. Das erklärt Artikel 4 Absatz 1. Darin wird erläutert, dass alle Informationen, welche eine identifizierbare, natürliche Person betreffen als personenbezogene Daten zu betrachten sind.

Die Verarbeitung der Daten beginnt schon mit der Erhebung der Daten, auch die Speicherung und Aufbewahrung sind eine Form der Verarbeitung der personenbezogenen Daten. Dazu kommt, dass die Daten nur zweckgebunden erhoben werden dürfen und nur mit Einwilligung der natürlichen Person. Dass alles muss nun geschützt und sichergestellt werden, nur wie?

Die schlauen Männer

War in der Beschreibung des Knotens nicht die Rede von „identifizierbar"? Warum also nicht einfach alle personenbezogenen Daten anonymisieren. Das wäre sicher eine Möglichkeit, um dafür zu sorgen, dass die Daten gesetzeskonform verarbeitet werden. Es gestaltet sich leider schwierig, Mitarbeiter Nummer 07857691 zu sprechen, wenn man nicht weiß, um welchen Mitarbeiter es sich handelt. Für Marktstudien und Kundenbefragungen ist das sicher der beste und einfachste Weg, aber für die Daten der Mitarbeiter und Kunden nicht. Firewall und Endpoint Protection sind sicher zwingend erforderlich, um zu verhindern, dass man von außen auf die Daten zugreifen kann. Sie nützen aber nichts, wenn der Hausmeister nach Feierabend durch die Personalakten scrollt.

Was ist mit der Zugriffssteuerung? Die Rechteverwaltung der Domäne ist ein großer Schritt, den Knoten zu lösen, aber es reicht noch nicht. Schließlich hat die IT-Abteilung, die für die Bereitstellung der Daten verantwortlich ist, noch immer den Nachschlüssel in der Hand.

Alexander der Große – oder besser: die Alexander die Großen

Wie so oft ist es nicht so einfach, das Problem mit nur einer Lösung zu beheben. Die schlauen Männer sind alle notwendig, wenn man die IT-Sicherheit und Vertraulichkeit wahren möchte, aber gelöst ist der Knoten erst, wenn auch die IT-Abteilung keinen Zugriff mehr auf die Inhalte der Daten hat. Wie schon erwähnt, muss das Rad nicht neu erfunden werden. Sie schützen ja bereits Ihre „Kronjuwelen".

Der Weg nach Asien

Wenn man dies alles betrachtet, ist eine Umsetzung heutzutage nur mit entsprechender Unterstützung von kompetenten Partnern möglich. Diesen Herausforderungen stellt sich beispielsweise die digitronic computersysteme gmbh mit ihren All-In-One Compliance-Paketen. □

Die Autoren

Peter Liebing ist Head of Sales & Marketing und **Alexander Schuschies** ist IT-Consultant bei der digitronic computersysteme gmbh. digitronic computersysteme ist ein deutscher Hersteller, wurde 1990 in Chemnitz gegründet und entwickelt seit 25 Jahren Software und Systeme für Kommunikation und IT-Sicherheit insbesondere für Großkunden.

DSGVO – Wie sorgen Kliniken am besten vor?

Wenn am 25. Mai 2018 die europäische Datenschutzgrundverordnung (DSGVO) in Kraft tritt, sind Unternehmen dazu verpflichtet, die darin festgelegten Datenschutzbestimmungen umzusetzen. Gelingt dies nicht, drohen hohe Bußgelder. Das gilt natürlich ebenso für Krankenhäuser. Gerade im Gesundheitswesen – beim Umgang mit besonders schützenswerten Daten – kommt es auf ein sorgfältiges Vorgehen an. Wie bereiten Kliniken sich also vor?

Von Dr. Ralf Rieken, Uniscon

Alarmierend ist, dass Prof. Dr. Thomas Jäschke, seit zehn Jahren Datenschutzbeauftragter für Unternehmen – insbesondere für Einrichtungen im Gesundheitswesen, im Hinblick auf Datenschutz und IT-Sicherheit im Gesundheitswesen zurzeit Folgendes beobachtet: „Datenschutz und Informationssicherheit werden in der täglichen Praxis oft nicht ausreichend berücksichtigt." Je kleiner die Organisation sei, desto weniger sensibel sei seiner Meinung nach der Umgang mit Daten. Manchmal könne sogar von „Gleichgültigkeit" gesprochen werden. Der Grund für die mangelnde Umsetzung in Datenschutz und in der IT-Sicherheit liege „in vielen Fällen an fehlender Unterweisung der Mitarbeiter", meint er im Magazin ExperSite.

Prof. Dr. Thomas Jäschke, Datenschutzbeauftragter für Unternehmen: „Datenschutz und Informationssicherheit werden in der täglichen Praxis oft nicht ausreichend berücksichtigt."

Das kommt auf Einrichtungen im Gesundheitswesen zu

Doch mit der DSGVO treten gleich mehrere Regelungen in Kraft, die eine ausgiebige Beschäftigung mit der Verordnung verlangen: Verschärfte Melde- und Informationspflichten, die Nachweispflicht, dass technischer Datenschutz („Privacy by Design") zum Einsatz kommt, Berücksichtigung des Standes der Technik, die Pflicht zur Datenschutz-Folgenabschätzung und hohe Bußgelder.

- Die in Art. 35 geregelte Datenschutz-Folgenabschätzung ist gänzlich neu. Sie ist für jede Tätigkeit durchzuführen, bei der personenbezogene Daten verarbeitet werden.
- Die Sicherheit der Verarbeitung muss unter Berücksichtigung des Standes der Technik entsprechend dem Risiko für die Betroffenen eingerichtet und nachgewiesen werden (Art. 32).
- „Privacy by Design": Datenschutz muss künftig von Anfang an nachweislich integraler

Während andere Cloud-Service-Anbieter organisatorische und technische Schutzmaßnahmen kombinieren, sind bei der Sealed Cloud auch die organisatorischen Maßnahmen durch technische ersetzt.

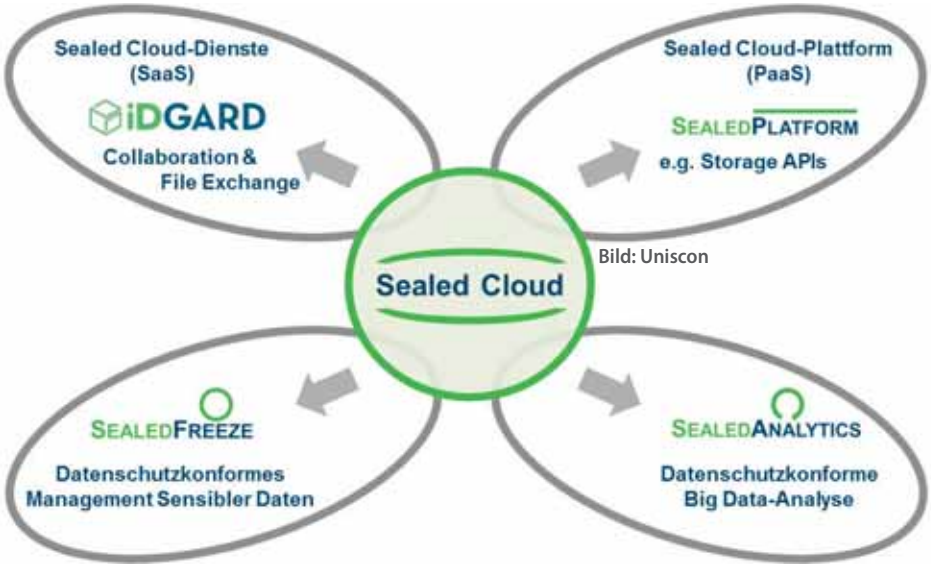


Bild: Uniscon

Bestandteil im Gestaltungsprozess der verwendeten Systeme sein (Art. 25).

- Die Verordnung erlaubt bei Verstößen Bußgelder in Höhe von vier Prozent des globalen Jahresumsatzes.

Wie erhalten Krankenhäuser Unterstützung?

Bereits heute findet man in jedem Krankenhaus einen Beauftragten für den Datenschutz. Diese sind maßgebend bei der Erstellung und Umsetzung der Datenschutz- und IT-Sicherheitskonzepte. Doch ist es nicht leicht, kontinuierlich auf dem Stand des Datenschutzrechts und der Sicherheitstechnik zu bleiben. Deshalb ist es wichtig, dass sie Hilfestellung bekommen. Eine Möglichkeit ist es, einen externen Datenschutzbeauftragten zu benennen, der sich speziell im Gesundheitswesen gut auskennt.

Einer, der die Angleichung von Theorie und Praxis anstrebt. Die Anforderungen sollten alltagsgerecht umgesetzt werden, um die eigentliche Tätigkeit nicht zu behindern. „Datenschutz darf kein Störfaktor sein", so Jäschke. Der Datenschutzbeauftragte sollte „unter Berücksichtigung der Verhältnismäßigkeit, Maßnahmen treffen, welche von den Mitarbeitern akzeptiert werden".

Um die Prozesse zu verbessern und IT-Kosten zu sparen, möchten auch Kliniken Cloud-Dienste nutzen. Doch die Beauftragung externer Dienstleister zur Verarbeitung von Daten ist, erklärt Dr. Hubert Jäger, IT-Sicherheitsexperte und Geschäftsführer des Cloud-Security-Unternehmens Uniscon, das zur TÜV SÜD Gruppe gehört, „eine unbefugte Offenbarung von Berufsgeheimnissen, die nach § 203 StGB strafbar ist". Dies sei bereits dann der Fall, wenn der Dienstleister potentiell Zugriff auf die Berufsgeheimnisse erlangen kann, nicht erst wenn er sich unbefugt Zugriff verschafft.

Dienste mit Sealed-Cloud-Technologie

Derzeit gibt es in Deutschland drei verschiedene Cloud-Dienste, die auf der Sealed-Cloud-Technologie basieren:

- **iDGARD (Uniscon GmbH)**
  Cloud-Dienst aus Deutschland für digitalen Datenaustausch und virtuelle Datenräume
- **uCloud (regio iT)**
  Dokumente zentral verwalten und teilen mit dem persönlichen und mobilen Datenspeicher der regio iT.
- **Die Versiegelte Cloud (Deutsche Telekom/ Magenta Security)**
  Der Cloud-Speicher mit der höchsten Sicherheit im Rechenzentrum der Deutschen Telekom.

Eine Ende-zu-Ende-Verschlüsselung der Geheimnisse verhindere dies weitgehend. Allerdings können bereits schon Verbindungsdaten Berufsgeheimnisse verraten, wenn ihre Verkettung mit öffentlichen Daten zu schützenswerten Informationen führt. In diesem Fall müssen auch sie laut Gesetz vor der Möglichkeit einer Kenntnisnahme durch den Dienstleister bewahrt werden (Metadatenschutz). Für Ärzte und Kliniken geeignete Dienste sind an einer entsprechenden Zertifizierung erkennbar, erklärt Jäger: „In der Regel wurden diese vom TÜV oder anderen akkreditierten Organisationen vergeben."

Bild: Uniscon

Dr. Hubert Jäger, IT-Sicherheitsexperte und Geschäftsführer bei Uniscon: „Die Beauftragung externer Dienstleister zur Verarbeitung von Daten ist eine unbefugte Offenbarung von Berufsgeheimnissen, die nach § 203 StGB strafbar ist".

DSGVO-Compliance: So löst es die Münchner WolfartKlinik

Die renommierte Münchner WolfartKlinik zum Beispiel suchte einen Cloud-Dienst zum Datenaustausch. Das Thema: „Als Klinik kommunizieren wir eng mit den ärztlichen Praxen, mit denen wir zusammenarbeiten", erzählt Tilmann Götzner, Geschäftsführer der WolfartKlinik. Er wollte das komplizierte VPN-Management und -Handling reduzieren und die Prozesse mit der Cloud-Lösung deutlich verschlanken.

Die WolfartsKlinik entschied sich nach längerer Suche für den Cloud-Dienst iDGARD der Uniscon GmbH. Der Grund dafür ist eine international patentierte Technologie, auf der dieser Dienst basiert: die Sealed Cloud. Während andere Cloud-Service-Anbieter organisatorische und technische Schutzmaßnahmen kombinieren, sind bei der Sealed Cloud auch die organisatorischen Maßnahmen durch technische ersetzt.

Sogar der Zugriff von Softwareanbietern, Hostern und Administratoren wird technisch ausgeschlossen – Stichwort „Betreibersicherheit". Die Daten sind auch während der Verarbeitung im Rechenzentrum geschützt: Alle Server stehen in gekapselten Segmenten. Bei einem Zugriffsversuch, werden die Daten automatisch in andere Segmente verschoben und vor Ort gelöscht (Data Clean-up). Technisch geschützt sind auch die Metadaten wie Inhalte und Verbindungsinformationen.

Sealed Cloud wurde nach dem „Privacy by Design"-Prinzip entwickelt und entspricht damit der DSGVO. Sie verfügt über ein Zertifikat der Schutzklasse 3 nach dem Trusted Cloud Datenschutzprofil (TCDP). TCDP konkretisiert die Normen ISO/IEC 27001/2 und ISO/IEC 27018. Die Bundesbeauftragte für den Datenschutz sowie alle Datenschutzaufsichtsbehörden der Länder haben die Zertifizierung bestätigt. □

Der Autor

Ralf Rieken ist Gründer und COO der Uniscon GmbH, einem Anbieter von hochsicheren Cloud-Lösungen. Er hatte verschiedene verantwortliche Positionen bei großen IT- und Netzlieferanten inne und lebte viele Jahre in den USA, wo er bis Ende 2007 als CEO eine Softwarefirma im Silicon Valley leitete. Zudem unterstützt er als Mitglied des Advisory Boards aktiv mehrere innovative IT-Firmen in Nordamerika und Israel.

Usable Security in der Softwareentwicklung

Warum ist Sicherheit in einer digitalen Welt so schwierig? Deutschland ist als Hochtechnologieland für seine hohe Produktqualität bekannt. Schließt dies Softwaresicherheit nicht mit ein? In der analogen Welt gibt es gute Beispiele, wie Sicherheit in jeglicher Form umgesetzt werden kann. Aus diesen lässt sich für die digitale Welt lernen.

Von Janosch Maier, Crashtest Security

Sicherheit wird vor allem dann als störend empfunden, wenn der Einzelne sich dadurch eingeschränkt fühlt. In Gebäuden mit besonderem Schutzbedarf soll kein Unbefugter Zutritt erlangen. Schleusen mit Sicherheitspersonal an jedem Eingang produzieren in Stoßzeiten Schlangen. Einfache Kontrollen mittels Key-Card können einfach durch Tailgating oder Piggybacking umgangen werden. Hier nutzt ein Unbefugter die Freundlichkeit der Menschen aus. Beispielsweise werden Firmenangestellte in vielen Fällen nach der Raucherpause ihren Rauch-Kameraden die Tür aufhalten. So kann ein Unbefugter meist unbemerkt – quasi Huckepack – mit durch die Tür schreiten. Wenn der Eingang nun eine geeignete Drehtür besitzt, kann immer nur eine – berechtigte – Person diese durchschreiten. Auch der noch so hilfsbereite, unbedarfte Mitarbeiter kann diese nicht offenhalten. So schränkt die Drehtür jeden einzelnen nur minimal ein und erhöht gleichzeitig die Sicherheit des Gesamtsystems.

Sicherheit muss einfach sein

In der digitalen Welt ist die Nutzbarkeit von Sicherheitsvorkehrungen noch wichtiger. Hier müssen Menschen mit unterschiedlichen IT-Kenntnissen Software bedienen können. Wenn erhöhte Sicherheit nun eine Barriere darstellt, wird diese ohne mit der Wimper zu zucken umgangen. So gibt es seit 1991 mit Pretty Good Privacy (PGP) eine Möglichkeit, verschlüsselte (und damit sicherere) E-Mails zu verschicken. Die Nutzung von PGP (und dessen Weiterentwicklungen wie GnuPG) ist jedoch so kompliziert, dass Edward Snowden seinem Journalisten-Kontakt ein zehnminütiges Erklärvideo dafür produzieren musste. Auf dem Screenshot (siehe Abbildung 1) ist alleine durch die Fülle der geöffneten Fenster zu sehen, warum das nötig war. In der Folge werden immer noch hauptsächlich unverschlüsselte E-Mails versendet. 25 Jahre nachdem eine Technologie zur Verschlüsselung verfügbar ist.

WhatsApp, einer der meistgenutzten Instant-Messenger-Dienste, schaffte es hingegen, eine ähnliche Art der Verschlüsselung für seine Nutzer einzuführen, ohne dass dies die Nutzbarkeit der Software änderte oder einschränkte. Das einzige, was die Nutzer davon mitbekamen, ist eine kleine Nachricht in jedem Chat, dass dieser nun verschlüsselt sei. Die Sicherheit ist also gar nicht das Problem, sondern die Art und Weise, wie diese implementiert wird.

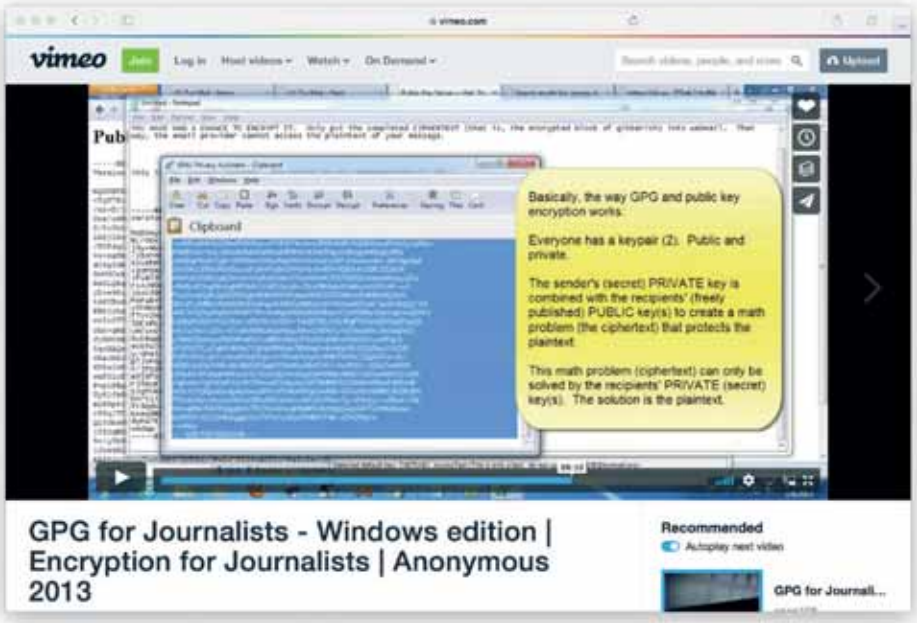


Abbildung 1: Ausschnitt aus dem Video GPG for Journalists

Bilder: Crashtest Security

Sicherheit in der Softwareentwicklung

Auch in der Softwareentwicklung darf Sicherheit die Entwickler nicht bei ihrer täglichen Arbeit behindern. Traditionell werden Sicherheitstests von einem manuellen Penetration Tester durchgeführt. Ein solcher wird beauftragt, wenn eine Anwendung fertiggestellt ist und kurz vor dem Release steht. Dieser benötigt mehrere Tage und testet die Anwendung auf die bekanntesten Sicherheitslücken (z.B. OWASP Top 10). Aufgrund der manuellen Arbeit dauert so ein Test relativ lange und ist teuer. Deshalb werden solche manuellen Penetration Tests häufig nur sehr unregelmäßig oder gar nicht durchgeführt. Bei der Art und Weise, wie früher Software entwickelt wurde – nach dem Wasserfall-Modell –, waren solche Tests ausreichend. Hier wurde nach einem langen Entwicklungszeitraum ein einmaliger Sicherheitstest durchgeführt und nach erfolgreichem Abschluss die Software zum Beispiel auf einer CD ausgeliefert. Wenn jedoch – wie heute – agil entwickelt wird, werden häufig mehrere neue Version pro Woche an die Kunden ausgeliefert. Dies passiert mit minimalen Kosten und teilweise ohne, dass die Nutzer dies bemerken – zum Beispiel, wenn eine Webseite aktualisiert wird. Für diese Art der Entwicklung sind unregelmäßige, manuelle Sicherheitstests nicht ausreichend.

Automatisierte Sicherheitstests

In den letzten Jahren haben sich bei der agilen Softwareentwicklung automatisierte Funktions-Tests auf unterschiedlichen Ebenen durchgesetzt und das Leben der Entwickler vereinfacht. Unit Tests überprüfen bei jeder Änderung der Code-Basis automatisch, ob der neu hinzugefügte Code seine vorgeschriebene Aufgabe erfüllt. Integrationstests, beispielsweise mit Hilfe von Selenium, testen im Vergleich ganze Abläufe mit Benutzereingaben, z.B. den Log-In-Vorgang, und überprüfen, ob die entwickelten Softwareteile einwandfrei miteinander agieren. Ein vollautomatisierter Test, welcher auf gängige Sicherheitslücken testet, hat sich jedoch aus mehreren Gründen noch nicht im Entwicklungsalltag durchgesetzt.

- Vielen Entwicklern fehlt es an IT-Sicherheitsexpertise sowie der Zeit sich einzuarbeiten, um Sicherheitstests für die eigene Software zu schreiben.
- Entwickler nutzen oft Frameworks, welche an sich die entwickelte Software sicherer

machen. Dies beruhigt die Entwickler, da sie durch die Frameworks anscheinend „sicher“ entwickeln. Jedoch werden die Sicherheitsfeatures der Frameworks oft umgangen, um bestimmte Features programmieren zu können, was die Sicherheit der Software extrem beeinträchtigt.

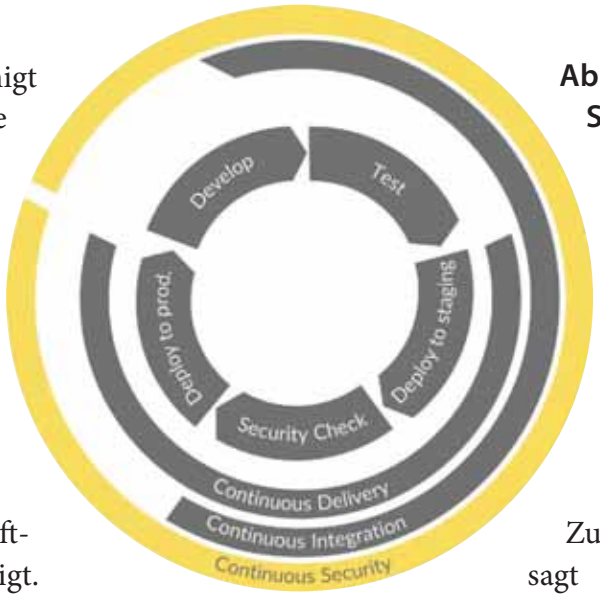


Abbildung 2: Continuous Security als Teil des agilen Softwareentwicklungsprozesses

- Manager verlassen sich darauf, dass ihre Entwickler genau wissen, was sie tun. Dass ein Entwickler jedoch nicht automatisch ein Sicherheitsexperte ist, wird selten bedacht.

Damit ein automatisierter Sicherheitstest in den Alltag der Entwickler integriert wird, muss dieser also so leicht zu verwenden sein wie ein Framework oder eine Programmbibliothek. Die Tests müssen benutzbar sein, also den Entwickler nicht bei der Arbeit stören. Außerdem müssen sie vollautomatisiert mit minimalem Konfigurationsaufwand zu verwenden sein. Hierfür gibt es mehrere Möglichkeiten, z.B. die Integration durch die Anbindung einer API (Application Programming Interface) mit dem Entwicklungssystem, welche jede Veränderung im Code registriert und nach erfolgreichen Unit- und Funktionstests einen Sicherheitsscan startet. Außerdem dürfen die Ergebnisse nicht in einem unübersichtlichen 300-Seiten-Report präsentiert werden, sondern müssen leicht verständlich mit konkreten Lösungsvorschlägen den Entwicklern gezeigt werden und per Ticketsystem Verantwortlichkeiten zugewiesen werden. Das ganze Testen muss kontinuierlich, während des gesamten Entwicklungszyklus der Software durchgeführt werden, um Lücken möglichst früh zu entdecken und beheben zu können. Nur so kann in der agilen Softwareentwicklung kontinuierliche Sicherheit gewährleistet werden (siehe Abbildung 2).

Zusammenfassend kann gesagt werden, dass Sicherheitsvorkehrungen nur dann verwendet werden, wenn sie benutzbar sind. In der Softwareentwicklung gilt dies auch für die Softwareentwickler, welche schon bei der Programmierung sicherstellen müssen, dass eine Software keine Schwachstellen aufweist. Sicherheitstests müssen dafür automatisiert und regelmäßig durchgeführt werden und die Entwickler dabei unterstützen, etwaige Fehler zu beheben. Auch bei der Gebäudesicherheit werden heutzutage schließlich Drehtüren und keine Burggräben, Zugbrücken und Fallgitter mehr verwendet. □

Der Autor

Janosch Maier ist Mit-Gründer und Geschäftsführer des IT-Sicherheits-Spezialisten Crashtest Security GmbH. Während seines Studiums der Informatik und der Pädagogik/Bildungswissenschaft entwickelte er ein Cyber Security Dashboard für das niederländische Justizministerium. Im Anschluss gründete er mit seinem Team die Firma Crashtest Security, welche Sicherheitstests für Webanwendungen automatisieren. Damit unterstützt er seine Kunden, ihre Web-Anwendungen vor Hacking-Angriffen zu schützen.

„Das war's noch nicht..."

Nach den jüngsten Cyber-Vorfällen durch WannaCry, Petya & Co wird derzeit die Angreifbarkeit der Automatisierungen in Produktionsanlagen und kritischen Infrastrukturen besonders intensiv in der Öffentlichkeit diskutiert. Diese Ransomware verschlüsselt wichtige Daten. Eine Freigabe dieser Daten erfolgt nur gegen Zahlung eines Lösegeldes (engl. ransom). In der Regel sind die Daten verloren. Von Stefan Menge, Achtwerk

Ransomware-Attacken sind eigentlich einfach zu verhindernde Angriffe, da eine bekannte Schwachstelle ausgenutzt wird. Ein Patchen, das heißt die Verwendung aktueller Software-Stände, hätte kein Eindringen zugelassen. Im Fall der Fälle hätte auch eine simple Maßnahme geholfen: das Rückspielen einer aktuellen, sauberen Datensicherung.

Aktuell stellen zielgerichtete Cyber-Angriffe (sog. Advanced Persistent Threats, APTs) durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer die höchste Gefährdung für Unternehmen dar. Das Ziel eines APT ist es, über eine längere Zeitdauer vertrauliche Informationen auszuspähen oder zielgerichtet Schaden anzurichten.

Industroyer – die neue Gefahr

Seit Neuestem sind Industroyer im Fokus von Sicherheitsexperten. Diese missbrauchen keine Lücken in den Steuerungs- und Automatisierungssystemen, sondern sprechen einfach in deren Sprache. Das heißt, dass sie die in Industrieumgebungen gängigen Kommunikationsprotokolle beherrschen. Dabei können Angreifer monatelang im Netzwerk aktiv sein und die notwendigen Informationen zusammentragen. Beispielsweise gehören Löschfunktionen zum Funktionsumfang, die sämtliche Spuren des Angriffs verwischen, Konfigurationsdateien löschen und das Betriebssystem des befallenen Windows-PCs in einen nicht-startfähigen Zustand versetzen. Diese komplexen Angriffsmethoden sind durch eine hohe Flexibilität und Dynamik gekennzeichnet. Die Erkennung solcher Cyberangriffe ist nur durch ein automatisiertes Monitoring des Datenverkehrs möglich. Durch die kontinuierliche Beobachtung werden Anomalien erkannt (Detektionsfähigkeit). Die Reaktionsfähigkeit bei einem Sicherheitsvorfall wird dann über eine umgehende Alarmierung im Unternehmen gewahrt.

Der Mehrwert und die Softfacts für eine Produktentscheidung

Neben den Diskussionen bezüglich Angriffen und Funktionen im Bereich Security gibt es einige weitere wichtige Aspekte, die in einer Gesamtbetrachtung nicht fehlen sollten.

Wenn sich jemand für eine Security Appliance entscheiden muss, stellt sich häufig die Frage nach der Herkunft. Sicherlich gibt es eine Reihe von Unternehmen, die nativ oder aus wirtschaftlicher Sicht den Stammsitz in den USA haben. Hier hat allerdings die Geschichte schon gezeigt, dass diese Lösungen nicht unbedingt in den entscheidenden Bereichen zum Einsatz kommen sollten.

Bild: Achtwerk

Leitstand mit IT-Netzüberwachung

„Security made in Germany“ ist deshalb gerade für die Produktion und Versorgungsunternehmen von unternehmenskritischer Bedeutung. So hat sich beispielsweise Achtwerk bewusst dafür entschieden, die Konzeption und Entwicklung der Lösung IRMA in Deutschland zu betreiben und auch in Zukunft deutsche Sicherheitsstandards zu gewährleisten.

Da in den sensiblen Strukturen der Automatisierung andere Anforderungen bei der Technologie und dem Personal vorliegen, sollte eine Sicherheitslösung eine sehr einfache Handhabung und einen sehr geringen Pflegeaufwand haben. Dieser Aspekt ist bei den meisten Security-Produkten eher vernachlässigt.

Um die Security-Anforderungen von vernetzten Automatisierungen schnell und effizient zu erfüllen, sollten Security-Produkte folgende Funktionen erfüllen:

Inventarisierung: Damit startet in der Regel das Gesamtprojekt. „Ich kann nicht schützen, was ich nicht kenne.“ Durch ein kontinuierliches Scannen des Netzwerkes muss jedes IT-Asset sofort erkannt, bestimmt und validiert werden.

Aussagekräftige Reports: Einstellungen sowie Listen sollten sich einfach in Reports ausgeben lassen. Denn diese aktuellen Ist-Zustände werden häufig für Besprechungen oder aktuelle Maßnahmen benötigt. Zudem sollten sich strukturierte Netzwerkdarstellungen einfach integrieren lassen.

Risiken bewerten: Jedes IT-Asset muss in einem integrierten Risikomanagement einfach bewertet werden können. Entsprechend können dann notwendige Maßnahmen schnell und einfach geplant und dokumentiert werden.

Überwachung des Netzwerkes: Jeder neue Teilnehmer muss unmittelbar erkannt werden. Servicemaßnahmen von externen Unternehmen lassen sich damit einfach kontrollieren, IT-Assets ohne Befugnis unmittelbar auffinden. Zusätzlich sollte die Sicherheitslösung über Filterkriterien verfügen, die eine schnelle Übersicht auf das Kommunikationsverhalten gewähren. Ein automatisiert erstellter Netzplan ist für den Anwender ein ideales Hilfsmittel zur Visualisierung seines Netzwerkes.

Alarmierung bei Unregelmäßigkeiten: Eine der wichtigsten Funktionen ist die Alarmierung. Reagiert das Netzwerk außerhalb der validierten Einstellungen, muss die Sicherheitslösung unmittelbar eine Information an die zuständigen Mitarbeiter versenden.

Kein Security-Produkt ohne **Update- und Supportkonzept:** Neben dem Updateservice sollte der Lösungsanbieter auch einen Support in unterschiedlichen Stufen bereitstellen. Damit zum Beispiel Berater, Systemhäuser wie auch Endkunden die optimal auf sie zugeschnittene Unterstützung erhalten. Und letztlich sollten Schulungen in regelmäßigen Abständen für eine lange und kontinuierliche Zusammenarbeit sowie zuverlässige Partnerschaft sorgen. □

Der Autor

Stefan Menge ist Geschäftsführer der Achtwerk GmbH & Co. KG, dem Hersteller der Industrie-Security-Appliance IRMA zur Identifikation von Cyberangriffen.

Die alten IT-Sicherheits-strategien haben ausgedient

Es zeigt sich zunehmend, dass in der Industrie 4.0 gängige IT-Sicherheitslösungen gegen Advanced Persistent Threats wie WannaCry und Industroyer keine Chance haben. Zum einen ist das Kind bereits in den Brunnen gefallen, bevor neue Sicherheitsupdates eingespielt werden. Zum anderen sind Firewalls & Co. in der Regel auch nicht mit Steuernetzumgebungen kompatibel. Es braucht eine Lösung, die jede Veränderung im Steuernetz sicher meldet und direkte Maßnahmen erlaubt.

Von Klaus Mochalski, Rhebo

WannaCry, Industroyer und NotPetya haben das Potential der Advanced Persistent Threats gezeigt. Sie fliegen unter dem Radar, nutzen Hintertüren und dringen von Firewall & Co. unbemerkt in Netzwerke ein. Sind sie einmal in diesem, haben sie freie Bahn. Denn weder Firewalls noch Intrusion Detection-Systeme (IDS) schauen in das Netzwerk. Sie sind nur Wächter an den Toren. Security Information and Event Management-Systeme (SIEM) überwachen zwar auch das Innenleben von Netzwerken. Sie sind jedoch häufig zu träge für kurzfristige Attacken. Zudem sind die genannten Lösungen in der Regel nicht kompatibel mit industriellen Steuernetzen.

Transparenz, Echtzeit und Integrationsfähigkeit zählen

Studien haben gezeigt, dass selbst die besten Firewalls in Kombination nur 95 bis 97 Prozent aller bekannten Gefahren abwehren. Von den unbekannten Gefährdungen wie auch Advanced Persistent Threats ist dabei noch nicht einmal die Rede. Für eine vollständige Absicherung, insbesondere im Zuge zunehmender Advanced Persistent Threats, bedarf es deshalb einer mehrstufigen Sicherheitsstrategie.
Die Ebene-1-Absicherung entspricht dabei einer hochwertigen, gut konfigurierten Firewall oder eines IDS, welche den Perimeter der Netzwerke überwacht und die bekannten Gefahren abwehrt. Darüber hinaus muss jedoch davon ausgegangen werden, dass Malware und Hacker die Ebene 1 erfolgreich unterwandern. Auf Ebene 2 setzt deshalb die industrielle Anomalieerkennung an. Sie übernimmt gleich mehrere Funktionen, um im Steuernetz vollständige Transparenz zu gewährleisten.

Cyber Asset Management

Mit dem Network Mapping und einer vollständigen Geräteinventur werden alle Netzteilnehmer eindeutig identifiziert und ihre Funktion (Master, Slave etc.) im Steuernetz analysiert. Bei dieser initialen Analyse lernt die Anomalieerkennung auch das standardmäßige Kommunikationsmuster, das im Steuernetz vorherrscht. Auf Basis dieses Musters

erfolgt die lückenlose Überwachung der Netzwerkkommunikation.

Echtzeiterkennung von Anomalien

Die Anomalieerkennung liest rückwirkungsfrei jegliche Kommunikation innerhalb des Steuernetzes mit und meldet Abweichungen vom Standardmuster. Die Abweichungen umfassen Cyberangriffe und Malware-Kommunikation, aber auch Qualitätsprobleme im Netzwerk durch z. B. Anlagenverschleiß, Fehlkonfigurationen und Kapazitätsengpässe. Dadurch wird ein Netzwerkmanagement erlaubt, dass weit über den Aspekt der reinen Netzwerksicherheit hinausgeht.

Mittels Deep Packet Inspection werden dafür alle Datenpakete bis auf Inhaltsebene analysiert. Wird eine Abweichung erkannt, wird diese in Echtzeit auf dem übersichtlichen Dashboard angezeigt. Die Daten der Anomalie werden vollständig und inklusive PCAP für die forensische Analyse gespeichert.

Priorisierung und Filterung

Den Meldungen werden automatisch Risikokategorien zugewiesen, um den Nutzer bei der Einschätzung der Gefahr zu unterstützen. Weiterhin können Anomalien nach individuell definierbaren Parametern gefiltert werden. Administratoren können so schnell die für ihr Steuernetz kritischen Anomalien herausfiltern und schnell auf die Vorfälle reagieren.

Integration

Lösungen wie Rhebo Industrial Protector erlauben die Integration der Anomaliedaten in die bestehenden Backend-Systeme wie MES oder Ebene-1-Systeme. Die Anomaliemuster externer Attacken können so zum Beispiel an eine Firewall übermittelt werden, um eine Wiederholung des Angriffs zu vermeiden. Das Sicherheitskonzept entwickelt sich damit zu einem selbstlernenden System.

Fazit

Die industrielle Anomalieerkennung gewährleistet Unternehmen der automatisierten Industrie und Kritischen Infrastrukturen somit vollständige Transparenz und eine lückenlose Überwachung aller Vorgänge in ihren Steuernetzen. Die priorisierte Datenvisualisierung beschleunigt eine effektive Umsetzung von Abwehrmaßnahmen. Über die Schnittstellen zu anderen Backend-Systemen wird die Nutzung der Steuernetzdaten für die Qualitätssicherung, die vorausschauende Instandhaltung und Prozessoptimierung reibungslos unterstützt.

Industrieunternehmen wissen somit stets, was in ihren Steuernetzen passiert und haben ein wirkungsvolles Werkzeug gegen Advanced Persistent Threats. □

Der Autor

Klaus Mochalski ist CEO der Rhebo GmbH. Er hat über zehn Jahre Erfahrung in der Entwicklung und Vermarktung von Technologien für Netzwerkmanagement und -sicherheit. Die von ihm mitgegründeten Firmen ipoque und Adyton Systems haben heute zusammen über 200 Mitarbeiter und wachsen weiter. Zuvor war Klaus Mochalski in Forschung und Lehre an internationalen Universitäten tätig.

Rhebo bietet Hardware- und Softwarelösungen sowie Auditservices, um in Kritischen Infrastrukturen und industrieller Automation das Gesamtsicherheitsrisiko zu verringern und die Produktivität zu erhöhen. Die IT-Marktanalysten von Gartner Inc. nennen Rhebo in ihrem aktuellen »Market Guide for Operational Technology Security 2017« als einziges deutsches Unternehmen, das eine Anomalieerkennung für industrielle Steuernetze anbietet.

Datensicherheit für das Internet der Dinge

Millionen von Webcams, Fernsehern, Druckern oder Maschinen verfügen heute schon über einen Internetanschluss. Aber nur wenige Hersteller kümmern sich um die Datensicherheit der Geräte. Das Internet of Things (IoT) gilt nach Ansicht vieler Experten als unsicher, die Privatsphäre der Nutzer ist nicht gewährleistet. Ohne großen Aufwand können Hacker mit speziellen Suchmaschinen die ungeschützten Geräte aufspüren und übernehmen. Von Michael Pickhardt, TDT AG

Ein Security-Hersteller hat aktuell IoT-Geräte untersucht und festgestellt, dass in Deutschland von 820.000 Netzwerken mit rund drei Millionen IoT-Geräten über 175.000 Geräte unsicher waren. Darunter 140.000 Router, das sind etwa 17 Prozent. In der Schweiz und in Österreich war die Quote der ungeschützten Router noch höher: Zwischen 33 und 40 Prozent aller Router hatten Schwachstellen. Für die Nutzer ist es schwer, die Sicherheit alleine herzustellen, hier ist die Industrie gefordert. Routerhersteller, die darauf vertrauen, dass die Kunden ihr Passwort nach dem Aufbau schon ändern werden, verhalten sich ebenso fahrlässig wie die Kunden, die aus Bequemlichkeit nichts unternehmen.

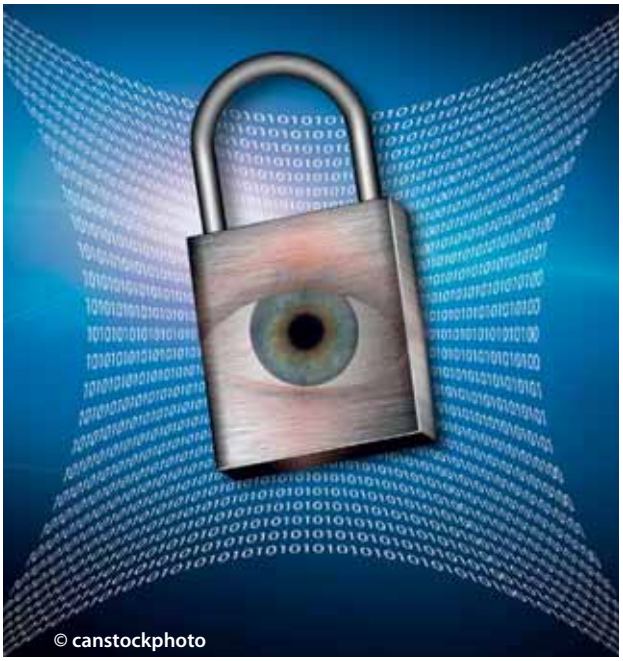
Sicherheitslücken in Routern

Die Anforderungen an Router im professionellen Bereich sind unabhängig vom Einsatzgebiet – vom Bankautomaten über die Filialvernetzung bis hin zur rauen Industrieanwendung – immer gleich: Höchste Sicherheit, maximale Verfügbarkeit, unterbrechungsfreie Datenübertragung.

Der Zugang zum Internet ist nach wie vor ein Haupteinfallstor in Unternehmensnetzwerke. Dabei werden keinesfalls nur Großunternehmen Opfer des kriminellen Datendiebstahls. Private Router werden ebenso gekapert wie solche von Verwaltungen oder mittelständischen Unternehmen. Unabhängig von der Anwendung gilt die Devise: Wer sich nicht kümmert, ist anfällig für Angriffe. Und mit der Zahl der vernetzten Geräte wächst auch die Gefahr, denn IoT-Geräte sammeln Daten und Informationen und bieten so ein Einfallstor. Meldungen über Sicherheitslücken in Routern sind alarmierend. Die Schäden reichen von Live-Bildern aus dem Kinderzimmer, über immense Telefonrechnungen durch manipulierte Zugänge bis hin zum Datendiebstahl.

Deutsche Unternehmen im Visier der Angreifer

Deutsche Unternehmen und ihre Produkte sind nach wie vor im Visier der ausländischen Konkurrenz. Schon lange kommen die Einbrecher nicht mehr mit dem Brecheisen, sondern sie



nutzen Sicherheitslücken in den IT-Systemen, um an die wertvollen Daten zu kommen. Jedes zweite deutsche Unternehmen erlebte in den vergangen zwei Jahren einen Spionageangriff oder einen Verdachtsfall, so eine aktuelle Studie zur Industriespionage. Aktuellen Schätzungen zufolge liegen allein in Deutschland die Schäden bei rund 50 Milliarden Euro jährlich.

VPN-Router als Schutz

Insbesondere im Small Office/Home Office-Bereich haben Hacker oft leichtes Spiel. Die als Zugaben für einen Internetanschluss mitgelieferten Router sind für den privaten Bereich – so sich die Nutzer um regelmäßige Updates kümmern – ausreichend, nicht aber für professionelle Anwendungen.

Die Gründe dafür sind vielfältig: Das Hauptargument ist die Sicherheit des eigenen Netzwerkes. Experten raten den Nutzern, generell alle vernetzten Geräte in einem VPN (Virtual Private Network) zusammenzufassen. Ein VPN gewährleistet eine sichere Kommunikation der verbundenen Geräte – auch über das Internet hinweg. Professionelle Router bieten hohe Verschlüsselungsstandards ebenso wie die Möglichkeit der Einrichtung von VPN-Netzwerken oder einer sicheren Zugangskontrolle über ein professionelles Netzwerkmanagement.

Im Wettlauf mit den Hackern sind die Anbieter von hochwertigen Routern durch erweiterte Schutz- und Kontrollfunktionen in ihrem System in der Regel immer einen Schritt voraus. Wie bei anderen Bedrohungen auch, hilft es nur bedingt, die Zäune und Hürden immer höher zu bauen, sondern es gilt, die Angreifer intelligent zu erkennen. Gleichzeitig braucht es eine hohe Sensibilität gegenüber dieser Art von virtueller Bedrohung.

Mit der zunehmenden Vernetzung und dem Austausch großer Datenmengen in der Industrie 4.0 steigen auch hier die Sicherheitsanforderungen. Die Anlagen und Produkte müssen ebenso wie die Daten und das Know-how verlässlich vor unbefugtem Zugriff geschützt werden. Als mittelständisches Unternehmen kennt TDT die konkreten Herausforderungen der Wirtschaft aus dem täglichen Geschäft: Sichere Datenübertragung und kompetentes Netzwerkmanagement sorgen dafür, dass die Daten der deutschen Wirtschaft nicht in falsche Hände geraten. □

Der Autor

Michael Pickhardt ist Vorstandsvorsitzender der TDT AG. Das mittelständische Technologie-Unternehmen entwickelt seit 1978 modernste Technik für die Datenkommunikation – beispielsweise High End VPN Gateways für die Hostumgebung, Industrie Class VPN-Zugangsrouter, Mobile Router für die 3/4G-Funknetze und Loadbalancer.

Impressum

Vogel IT-Medien GmbH
August-Wessels-Str. 27, 86156 Augsburg
Tel. 0821/2177-0, Fax 0821/2177-150
eMail redaktion@vogel-it.de

IT-BUSINESS

Redaktion: Wilfried Platten/pl (-106) – Chefredakteur, Dr. Andreas Bergler/ab (-141) – CvD/ltd. Redakteur

Co-Publisher: Lilli Kos (-300)
(verantwortlich für den Anzeigenteil)

Account Management:
Besa Agaj/International Accounts (-112),
Stephanie Steen (-211),
Hannah Lamotte (-193)
eMail media@vogel-it.de

SECURITY-INSIDER.DE

Redaktion: Peter Schmitz/ps (-165) – Chefredakteur, Jürgen Paukner/jp (-166) – CvD

Co-Publisher: Markus Späth (-138), Tobias Teske (-139)

Key Account Management: Brigitte Bonasera (-142)

Anzeigendisposition: Dagmar Schauer (-202)

Grafik & Layout: Brigitte Krimmer, Johannes Rath, Udo Scherlin, Carin Böhm (Titel)

EBV: Carin Böhm, Brigitte Krimmer

Anzeigen-Layout: Johannes Rath

Adressänderungen/Vertriebskoordination:
Sabine Assum (-194), Fax (-228)
eMail vertrieb@vogel-it.de

Abonnementbetreuung: Petra Hecht, DataM-Services GmbH, 97103 Würzburg
Tel. 0931/4170-429 (Fax -497)
eMail phecht@datam-services.de

Geschäftsführer: Werner Nieberle – Geschäftsführer/Publisher

Druck: deVega Medien GmbH, Anwaltinger Straße 10, 86156 Augsburg

Haftung: Für den Fall, dass Beiträge oder Informationen unzutreffend oder fehlerhaft sind, haftet der Verlag nur beim Nachweis grober Fahrlässigkeit. Für Beiträge, die namentlich gekennzeichnet sind, ist der jeweilige Autor verantwortlich.

Copyright: Vogel IT-Medien GmbH. Alle Rechte vorbehalten. Nachdruck, digitale Verwendung jeder Art, Vervielfältigung nur mit schriftlicher Genehmigung der Redaktion.

Nachdruck und elektronische Nutzung: Wenn Sie Beiträge dieser Zeitung für eigene Veröffentlichung wie Sonderdrucke, Websites, sonstige elektronische Medien oder Kundenzeitschriften nutzen möchten, erhalten Sie Informationen sowie die erforderlichen Rechte über www.mycontewntfactory.de, Tel. 0931/418-2786.

Manuskripte: Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Sie werden nur zurückgesandt, wenn Rückporto beiliegt.

Vogel Business Media

Vogel IT-Medien, Augsburg, ist eine 100prozentige Tochtergesellschaft der **Vogel Business Media**, Würzburg, einem der führenden deutschen Fachinformationsanbieter mit 100+ Fachzeitschriften, 100+ Webportalen, 100+ Business-Events sowie zahlreichen mobilen Angeboten und internationalen Aktivitäten. Seit 1991 gibt Vogel IT-Medien Fachmedien für Entscheider heraus, die mit der Produktion, der Beschaffung oder dem Einsatz von Informationstechnologie beruflich befasst sind. Dabei bietet er neben Print- und Online-Medien auch ein breites Veranstaltungsportfolio an.

Die wichtigsten Angebote des Verlages sind **IT-BUSINESS, eGovernment Computing, IP-Insider.de, Security-Insider.de, Storage-Insider.de, CloudComputing-Insider.de, DataCenter-Insider.de, Dev-Insider.de** und **BigData-Insider.de.**

Inserenten

G DATA Software AG	Bochum	https://www.gdata.de/	2, 8, 9
NCP engineering GmbH	Nürnberg	https://www.ncp-e.com/de/	34, 35, 68
netfiles GmbH	Burghausen	https://www.netfiles.de/	14, 15
secunet Security Networks AG	Essen	https://www.secunet.com/	5, 22, 23
Virtual Solution AG	München	http://virtual-solution.com	30, 31
Vogel IT-Akademie	Augsburg	http://www.akademie.vogel-it.com/	67

IT-SECURITY
MANAGEMENT & TECHNOLOGY
CONFERENCE 2018

EXPERTENFORUM | BEST PRACTICES | KNOW-HOW | NETWORKING

SAVE THE DATE!

Geplante Termine und Orte:

21.06.2018 München
28.06.2018 Köln
03.07.2018 Hamburg
05.07.2018 Frankfurt

Jetzt vormerken unter **www.itsecurity-conference.de**

Eine Veranstaltung der **Vogel** IT-Akademie

NCP
SECURE COMMUNICATIONS

Sicherheit
in Ihrer Hand

Die professionellen VPN Clients für iOS, Android, macOS und Windows.

Die NCP Secure Enterprise Clients für Smartphones, Tablets und Co. schaffen eine hochsichere VPN-Verbindung zu zentralen Datennetzen von Firmen und Organisationen. Der neue NCP VPN Client für iOS regelt mit VPN On Demand den automatischen Aufbau des VPN-Tunnels und die ausschließliche Kommunikation darüber.

Ihre Vorteile mit NCP Secure Enterprise Clients:

- Zentrale Verwaltung über das NCP Secure Enterprise Management
- Personal Firewall
- Starke Authentisierung
- Load Balancing
- Fallback IPsec / HTTPS (VPN Path Finder Technology)

Next Generation Network Access Technology

Sicherheit made in Germany

Secur|Ty made in Germany

Jetzt informieren!