



@-yet:

"Das ITSIG 2.0 in der Anwendungspraxis am Beispiel eines Unternehmens der Automatisierungstechnik"

IT-Sicherheitsrechtstag des TeleTrust , 24. September 2021

@YET

@-yet Fakten: seit 2002 für Digitale Souveränität im Einsatz

@YET

Gegründet 2002

seitdem inhabergeführt

Sitz in Leichlingen NRW

Über 50 Mitarbeiter:innen

in Deutschland und weltweit tätig

Family Offices

Mittelständler

Konzerne

Organisationen

**IT-Sicherheit ist nicht
alles, aber alles braucht
IT-Sicherheit.**



Produktion, Vertrieb, Verwaltung, HR, Logistik, Marketing etc.:

**Es gibt keinen Unternehmensteil,
dessen Funktionieren und Erfolg nicht
von unterschiedlichen Aspekten der
IT-Sicherheit abhängig wäre.**



Digitale Souveränität durch IT-Sicherheit

Die Lage!

Wie ernst ist es denn wirklich?

**Oder soll nur Panik gemacht
werden?**

Bei uns ist noch nie
was passiert!

Das wissen Sie gar nicht.
Wahrscheinlicher ist:
Sie haben es nicht bemerkt.

Oft gehört

@YET

Es gibt sowieso keine
100%-ige Sicherheit!

Ja, so ist das.

Aber Resignation ist keine
Option.

Wer sollte uns denn
angreifen?
Wer interessiert sich
denn für uns?

Wettbewerber aus dem
In- und Ausland

Organisierte
Kriminalität

Innentäter

Staaten

Terroristen

Was sind die Motive?

1. Geld

2. Know-how

Rache und
"beleidigt sein"

"Spaß am Hacken"

Sabotage

u.v.m.

So ist es leider:

**Die Risiken nehmen zu.
Die Bedrohungslage ist ernst.
Es kann jeden treffen.**



So ist es leider:

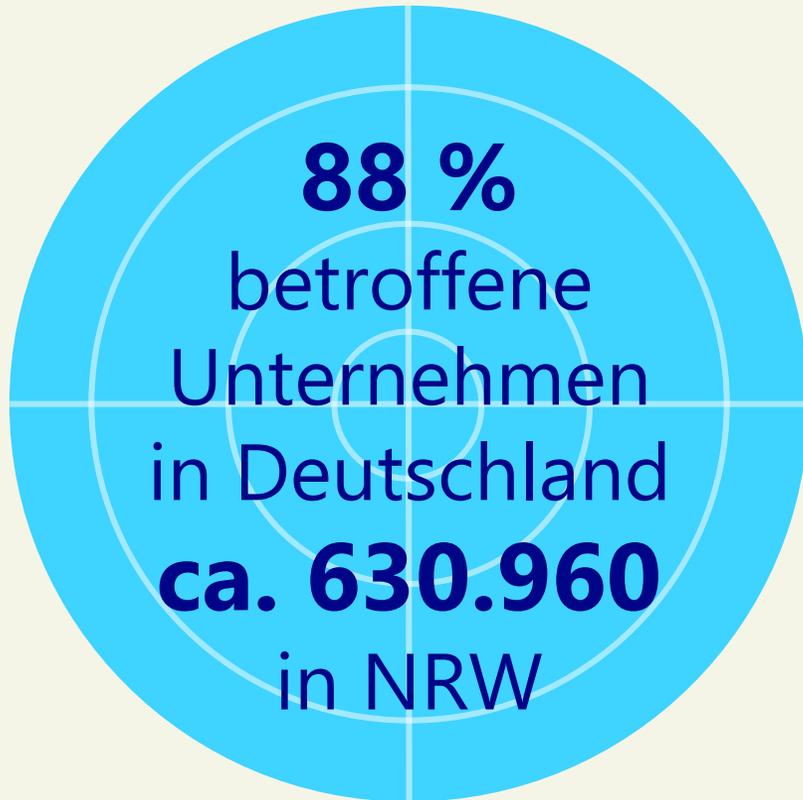


Cybercrimeumsätze übertreffen Drogenumsätze

Aktuelle Zahlen:

Quelle: bitkom Research 2021

@YET



@-yet Forensiken seit 2019

@YET



große + kleine Vorfälle

teils ganze Konzerne bis

häufig durch technische Lücken
ausgelöst

häufig erfolgreiche Phishingattacken

sehr viel Ransomware / Erpressung

zeitliche Entwicklung Cyberattacken



Und wie machen die das?

Klassisches Hacking von außen

ET

Datenträger und Geräte stehlen

Whistle-Blower:innen

Informationen von innen: strukturelle Schwächen, Social Engineering etc.

Ausnutzen von Sorglosigkeit beim Surfen

Über infizierte Websites, Portale, Apps – Desktop und Mobile

Datenabfluss (Klau) durch (Ex-)Mitarbeiter:innen

True Cybercrime – aus den Akten von @-yet:

Die typischen Vorgehensweisen



Es ist nicht wie im Film:
Hacker im Hoodie, die in
irgendwelchen Kellern sitzen
und aus sinistren Motiven
Chaos verbreiten wollen.

@YET

Es sind top-organisierte
Gruppen von Profis. Hacking
ist der Job, mit dem sie ihre
„Brötchen“ verdienen. Und
das machen die mit
höchster Professionalität
und Arbeitsteilung



Die einen suchen die Lücken in Systemen, Anwendungen, Protokollen und verkaufen diese

Wieder andere schreiben sogenannte Exploits - Software, die die Lücken ausnutzen und verkaufen diese

Und wieder andere greifen an, verschlüsseln und erpressen

Ausspähen und angreifen.

Permanente Suche nach Schwachstellen in von außen sichtbaren technischen Schwachstellen in Systemen, Firewalls, Webanwendungen, IOT's etc.

Scans laufen unablässig und vollautomatisiert durchs WWW und suchen ungepatchte Lücken

Wird eine Lücke gefunden, wird automatisch der entsprechende Exploit „nachgeschoben“

Dieser Exploit „öffnet“ das Firmennetz für den Angreifer. Er geht rein und zunächst auf „Tauchstation“

Ausspähen und angreifen.

Gründliche und gezielte Recherche von Personen, E-Mail-Adressen, sonstige personenbezogene Informationen auf Firmenwebseiten, in SocialMedia Umgebungen, sonstige Quellen im (dark-)net

Phishing E-Mails mit verdorbenen Anhängen (PDF, Excel – egal) oder Links zu gefakten Seiten.

Einspielen eines Exploits

Dieser Exploit „öffnet“ das Firmennetz für den Angreifer. Er geht rein und zunächst auf „Tauchstation“

Austricksen und angreifen.

Ein USB-Stick auf dem Parkplatz.
Ein USB-Stick als Give-away auf der Messe
etc. pp.

Der USB Stick wird in den eigenen Rechner
gesteckt – und der Rest passiert von selbst

...

USB Blocker werden oft ausgehebelt – der
infizierte Stick simuliert eine Tastatur oder
Maus

Ein Exploit „öffnet“ das Firmennetz für den Angreifer.
Er geht rein und zunächst auf „Tauchstation“

True Cybercrime – aus den Akten von @-yet:

Incident Response: Ransomware und Erpressung – der Fall Pilz

Was war passiert?



Die Angreifer konnten mit einer Malware eindringen und per Datenverschlüsselung das Unternehmen lahmlegen.

Kompletter weltweiter Stillstand von IT und Produktion.

Kommunikationsstillstand: kein E-Mail, keine VOIP-Telefonie, Firmenhandys via MDM gelöscht.

Ziel Erpressung: "Geld gegen Schlüssel."

Die Angreifer hielten sich zur Planung und Vorbereitung ca. 5 Monate unbemerkt im Firmennetzwerk auf.

Was war passiert?



Erstzugriff wahrscheinlich Mai 2019

Start der Verschlüsselung am
11.10.2019

Leider analyse- und
ermittlungskontraproduktive
Sofortmaßnahmen

Löschen, Neustarten, Neuaufsetzen
von Systemen vernichtet Spuren

Alles steht

Vorgehen Pilz



Thomas Pilz realisiert, dass der IT-Dienstleister und seine eigene IT mit der Situation nicht klarkommen

er ruft Sonntagnachmittag, den 12.10.2019, gegen 16 Uhr @-yet an

@-yet beginnt mit den Arbeiten in den frühen Morgenstunden des 13.10. mit zunächst 3 Forensiker

Im Laufe der Woche(n) Aufstockung auf bis zu 10 Leute

Versuch Behörden und BSI um Hilfe anzugehen – zunächst erfolglos

Vorgehen



Organisation IT-Krisenteam

- Pilz GF/@-yet PL
- @-yet Forensiker
 - Pilz IT
- Kripo Esslingen

Analyse Backups

- ### Analyse Systeme:
- alle Windowssysteme betroffen
 - nicht alle Linuxsysteme

Vorgehen



Analyse der Netze und aller
Endsysteme:

- Suche nach Patient Zero
- Suche nach IOCs mittels
Spezialscanner

PILZ informiert

- Mitarbeiter
- Kunden
- Partner
- Behörden (Kripo, Datenschutz)

Vorgehen



Backups:
- Bis 6 Monate zurück alle zerstört!!

Die Angreifer hielten sich zum Zeitpunkt der Verschlüsselung ca. 3 Monate im Netzwerk auf

Das Netzwerk wurde umfänglich erkundet und man hat sich die benötigten Berechtigungen „erarbeitet“

Die Angreifer haben auch das „AntiVirus“ manipuliert

Vorgehen



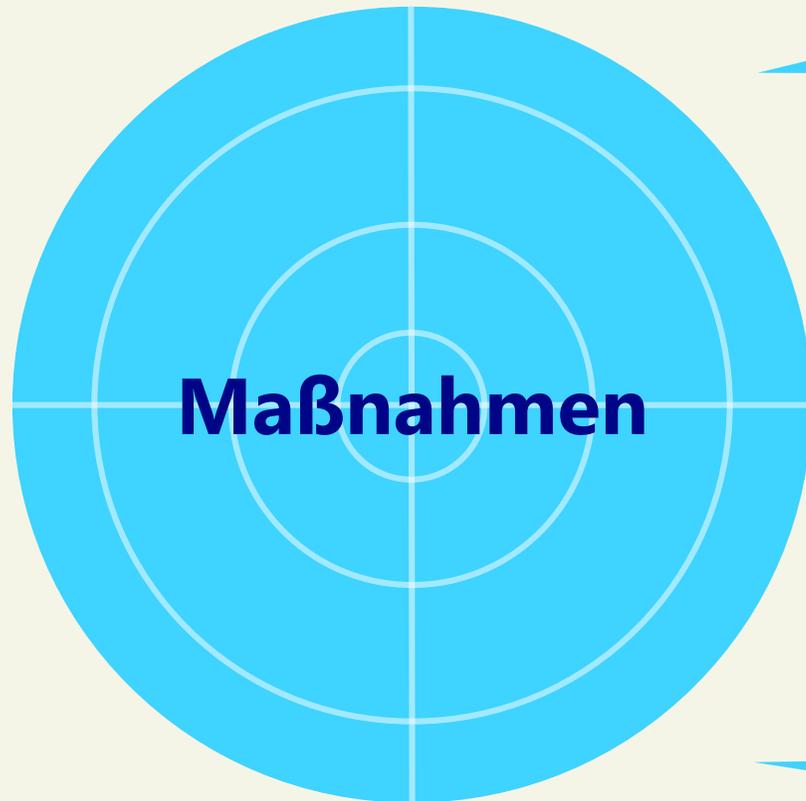
Alle Accounts der regulären Domänen-Administratoren wurden gesperrt (ein Account mit delegierten Admin-Rechten wurde übersehen)

Einige Netzwerk Speicher Systeme (NAS) wurden gelöscht

Vorgänge gestartet, die den Zugriff auf Backups erschweren

„Verschlüsselungskomponente“ wurde strategisch manuell auf bestimmten Systemen ausgeführt (z.B. Antivirus als erstes)

Vorgehen



Nach 1 Woche Entscheidung:
Neuaufbau der IT

Neuaufsetzen aller zentralen
Server- und Stagesysteme

Scannen und bereinigen aller
Clients und sonstigen Endgeräte

Weitere forensische Analysen

Engste Abstimmung mit Kripo, LKA,
FBI!

Vorgehen



Nach 5 Wochen liefen erste zentrale Anwendungen wieder

Nach 6 Monaten waren alle in allen Ländern wieder voll arbeitsfähig

Insgesamt hat es nahezu 1 Jahr gedauert bis der „alte“ Komfort, nur diesmal in „sicher“ wieder hergestellt war

Ende 2020 konnte der bitpaymer nicht zuletzt durch die Analysen bei PILZ unschädlich gemacht werden

Vorgehen



Nach 5 Wochen liefen erste zentrale Anwendungen wieder

Nach 6 Monaten waren alle in allen Ländern wieder voll arbeitsfähig

Insgesamt hat es nahezu 1 Jahr gedauert bis der „alte“ Komfort, nur diesmal in „sicher“ wieder hergestellt war

Ende 2020 konnte der bitpaymer nicht zuletzt durch die Analysen bei PILZ unschädlich gemacht werden

Wie wurde geholfen?



**Mittelständler
produzierend
international tätig
> 2.500 MA**

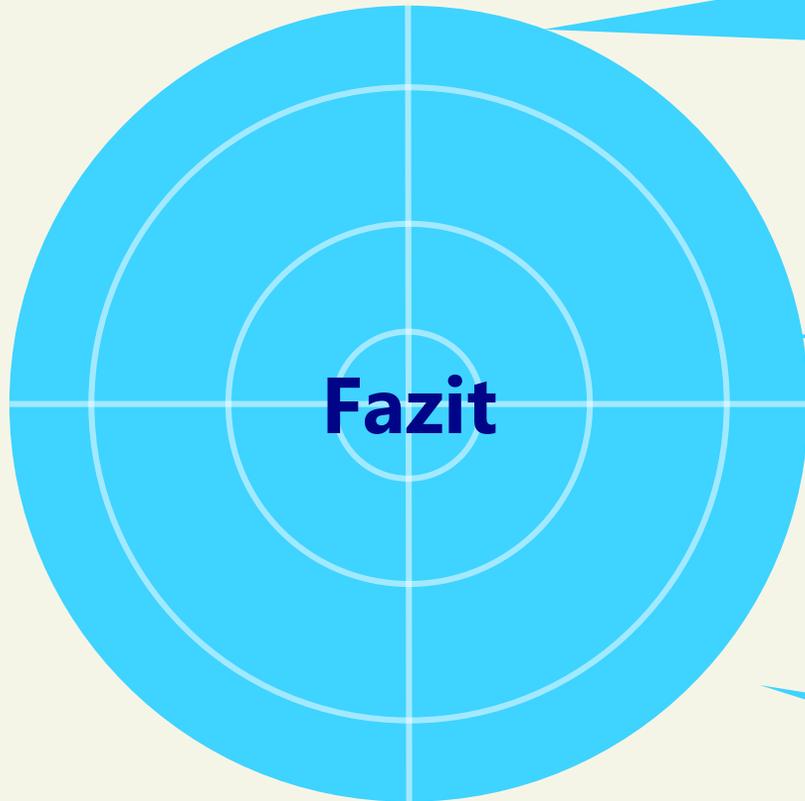
Freitagabend Angriff, Info an @YET
leider erst am Sonntagnachmittag
Montagmorgen um 6 Uhr war @YET
vor Ort

Die zuständigen Ermittlungsbehörden
wurden ins Boot geholt – Kripo, LKA,
bis hin zum FBI.

Lösegeld wurde nicht gezahlt, IT und
Betrieb konnten sukzessive vom
Trojaner befreit werden und den
Normalbetrieb wieder aufnehmen.

Die @YET Abwehr- und Forensikarbeit
trug dazu bei, dass die Angreifer-
Gruppe zerschlagen werden konnte.

Wie konnte das passieren?



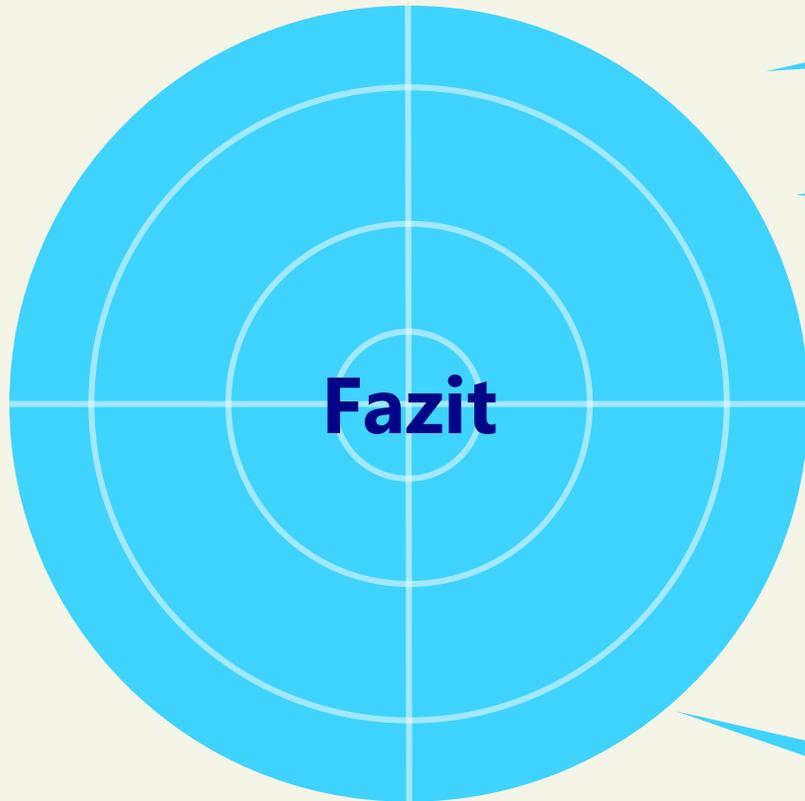
Zum einen:
- ein schlecht implementierter Basisschutz
- chaotisch unstrukturierte Infrastruktur
- keine ausreichende Notfallorganisation

Das Einfallstor konnte nicht final ermittelt werden:
Home Office / Phishing / via Dienstleister / per IOT?

Der Grund: Systeme wurden vorschnell neu gestartet, neu installiert, Daten gelöscht, Spuren dadurch vernichtet.

Unternehmen und IT-Dienstleister waren nicht ausreichend vorbereitet

Fazit.



Das Unternehmen hat den Angriff überlebt.
Aber zu einem hohen Preis.

Mit der richtigen Prävention, einem ISMS,
vor allem aber einer sicheren IT-
Infrastruktur wäre für es für die Angreifer
schwerer gewesen

Eine Bedrohung – bitpaymer - ist
verschwunden. Viele weitere
Ransomwares und ihre Absender treiben
weiter ihr Unwesen und richten täglich
Schaden an.

Die Zusammenarbeit mit Kripo und Co war
sehr gut und extrem hilfreich

**@YET Fazit aus
vielen Fällen:**

**Machen Sie sich digital souverän
und bleiben Sie erfolgreich.
IT-Sicherheit ist ein wichtiger
Schritt dorthin.**

Dafür gelten die 5 @-yet Grundsätze der IT-Sicherheit



1. Lieber den Ernstfall verhindern als den Ernstfall überstehen

Schwachstellenanalyse, Angriffssimulationen, physikalische Integrität, Code-Überprüfung.
Wir testen alles, was es zu testen gibt und bauen nachhaltig Resilienz auf.

2. Bewegliche Ziele sind schwerer zu treffen

Ein neues Schloss und fertig? IT-Sicherheit ist keine Einzelmaßnahme, sondern ein Prozess. Wir geben Ihnen das Rüstzeug, damit Sie in Zukunft sicherer arbeiten und leben können.

3. Im Schadensfall zählt jede Sekunde

Wenn es brennt, wartet man nicht ab, ob das Feuer von alleine ausgeht. Unsere Expert:innen sorgen dafür, dass der Betrieb so schnell und sicher wie möglich weitergehen kann.

4. IT-Sicherheit fängt beim Menschen an

Die größte Schwachstelle ist nicht im, sondern vor dem Rechner. Wir klären auf, sensibilisieren, bilden weiter, führen Notfallübungen durch, damit Ihre Mitarbeiter:innen sich sicher fühlen und sicher handeln.

5. Besser, wenn man die besten Leute auf seiner Seite hat

Nur absolute Expert:innen, die mit allen Wassern gewaschen sind und jeden Trick kennen, holen für Ihr Unternehmen das optimale Ergebnis. Das sind wir.

**Und wenn trotzdem
etwas passiert oder
auffällig erscheint?**

Auch dann gilt

**Don't
Panic**



**@YET
anrufen**

**Das wars
von meiner Seite**



@YET

Kontakt

@-yet GmbH

Schloss Eicherhof
42799 Leichlingen

+49 2175 16 55 0
info@at-yet.de

Kontakt

Wolfgang Straßer

Das @-yet Leistungsspektrum im Schnelldurchlauf



Prevention

Check IT-Resilienz

- Quick Check
- Penetrationstesting
- Red Teaming
- Threat Hunting
- Cloud Security
- Mobile Device Security
- Web- und Mobile Application Check
- Code Review
- WLAN / WiFi-Security

Check physische Sicherheit

- Gebäude- und Geländecheck

Check Human Factor

- Social Engineering Training
- Security Awareness & Live Hacking
- Phishing Kampagnen
- Open Source Intelligence (OSINT)

Check Strukturen und Prozesse

- Organisations- und Regelanalyse
- Zertifizierungsbegleitung



Continuity

- Business Impact Analyse
- Risiko-Assessment und Risiko-Management
- Hochverfügbarkeit



Compliance

- DS-GVO-Prüfung
- Externe:r Datenschutz-beauftragte:r
- Datenschutz-Management
- Schulungen Datenschutz



Notfallhilfe

- Analyse von Sicherheits-vorfällen
- Incident Response
- Digitale Forensik
- Prüfung auf Systemintegrität
- Threat Hunting
- Data Recovery



Beratung

ISMS

- ISO27001/VDS/BSI
- CommonCriteria
- TISAX
- etc.

Sichere IT-Infrastruktur

- Netzsicherheit
- sichere Kommunikation
- Hardening
- Endpointsicherheit
- etc

Sicherer IT-Betrieb

Sichere Anwendungen

- SecureCoding
- CodeReview
- etc.

Sicher in die Cloud

Der Sicherheitsvorfall

- was tun und was lassen?
- wen ansprechen?
 - Intern
 - extern