

TeleTrust-interner Workshop

Essen, 29./30.06.2017

Bedürfnisse von Großanwendern

Sebastian Barchnicki

Hintergrund Masterarbeit

"Möglichkeiten und Wege einer Kooperation von Großanwendern und IT-Sicherheitsindustrie für ein höheres notwendiges Maß an IT-Sicherheit und Vertrauenswürdigkeit"

- In Kooperation und breiter Unterstützung durch
 - TeleTrust - Bundesverband IT-Sicherheit e.V.
 - VOICE – Bundesverband der IT-Anwender e.V.
 - ASW e.V.

- Intensive Diskussion mit CIOs/CISOs der DAX 30 (Katalogumfang: 18 Seiten, 8 Kapitel, ~1,5h/Gespräch)








Umfrage im Rahmen der Masterarbeit

„Möglichkeiten und Wege einer Kooperation von Großanwendern und IT-Sicherheitsindustrie für ein höheres notwendiges Maß an IT-Sicherheit und Vertrauenswürdigkeit“

an der Westfälischen Hochschule Gelsenkirchen in Kooperation mit dem Bundesverband IT-Sicherheit e.V. (TeleTrust). Ziel dieser wissenschaftlichen Umfrage sind Großanwender und insbesondere DAX30-Unternehmen mit dem Hauptsitz in Deutschland.

Wer ist der TeleTrust?

TeleTrust – Bundesverband IT-Sicherheit e.V., gegründet 1989, ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Beratung, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst.

Ziel des Verbandes ist insbesondere die Förderung der Vertrauenswürdigkeit von Informationstechnologien und Kommunikationstechnik.

Masterand/Autor: Sebastian Barchnicki
Betreut durch: Prof. Dr. Norbert Pohlmann

Unternehmen:	
Interviewte Person(en) & Position:	
Datum:	
Ort:	

Motivation

Die Zielgruppe (Großanwender) einmal genauer nach ihren Befindlichkeiten, Denkweisen, Meinungen und Wünschen im Detail zu befragen

Danke! **DAX30**

- 12 DAX Konzerne haben sich sehr viel Zeit genommen :-)

 - Insgesamt wurden 216 Seiten Fragen ausführlich behandelt zu:
 - Ihr Unternehmen/Zahlen, Beschaffung, Einsatz, Allgemeines, Markt & Defizite, Kooperation, Sympathien, Last Words
- ➔ Hochspannender Einblick in die Arbeit, Bedürfnisse und Situation der DAX30**

Auszüge

Nachfolgend einige Auszüge im Hinblick auf die laufende Erarbeitung von Ergebnissen.

"Ihre Schwerpunkte bei IT-Sicherheit?" - "Nicht einfach zu beantworten"

- Awareness
- Infrastruktur
- Cloud
- Forensik & Pentesting
- Incident Management
- IAM (Identity Access Management)
- Cyber Defense Center
- Vulnerability Management
(Realtime-Monitoring inkl. APT-Handling)
- Source Code Bewertung (in internen Projekten)

Die größten Ängste und Bedrohungen?

- Cyberwar/Cybercrime
- Angriffe durch Geheimdienste
- Angriffsvektor Benutzer (Awareness)
- Einzug von AI in den Angriffssektor
- Disruptive und agile Digitalisierung ohne Plan
- Stärkere Professionalisierung der Angreifer durch (leichten) Einkauf von *Diensten*
- Möglicher steigender Aufwand für die Verteidigung

Gemeinsam ist es einfacher

- In jedem Fall wird die Idee einer Zusammenarbeit grundsätzlich sehr begrüßt

- Geäußerte Ideen hinsichtlich einer möglichen Zusammenarbeit:
 - Über Verbände, da keine 1:1 Kommunikation
 - Konferenzen und Workshops inkl. Behörden
 - Sehr zielgerichtete Interviews/Fragebögen
 - ...

- Die Begegnung auf Augenhöhe ist eine gute Idee

"Was nervt Sie bei dem Gedanken an IT-Sicherheitsprodukte?" – Zitat:

- **Halten nicht, was sie versprechen**
- schwarz/weiß -> entweder sicher oder nicht, Grautöne fehlen
- Dass DE nicht in der Lage ist, Digitale Souveränität zu erzeugen!
- **Alles ist kompliziert**
- neue Projekte = Aufwand immens groß (Rollout) & Komplexität bei der Implementierung
- **Usability**
- Keine *IT-Replaceability*
- *Und VIELE mehr*

"Was ist das aller wichtigste, das Sie von einer IT-Sicherheitslösung erwarten?" – Zitat:

- **Verlässlichkeit**
- **Performance, Transparenz + "Smoothness"**
→ Nutzer sollten es gar nicht wahrnehmen
- **Behindert nicht das Business**
- **Resilienz**
- **Qualität**
- **Hält was sie verspricht**
- **Den CISO Job erleichtert**
- **Das sie FUNKTIONIERT! ;-)**

Technologiesprünge

"Sind Sie Bereit größere Technologiesprünge zu machen?"

- JA!
- (grundsätzlich)

Einschränkung für höhere Sicherheit

"Ist eine größere Einschränkung der Nutzer durch Reduktion von Freiheitsgraden (Hochsicherheitsprodukte) = höhere Sicherheit in Ihrem Unternehmen durchsetzbar?"

- (Grundsätzlich) JA!
- Jedoch nicht überall

"Was ist das allerwichtigste, das Sie von einem IT-Sicherheitsanbieter erwarten?" – Zitat:

- Kompetenz
- Vertrauenswürdigkeit
- Zurückhaltung
- Versteht die Probleme des CISO und hilft ihm
- exzellenter Support weltweit
- Ehrlichkeit, Schnelligkeit, Flexibilität
- Langfristige Partnerschaften
- Unerwünscht: Anbieter klopft direkt beim Management

"Last Words" oder was Ihnen die DAXe unbedingt sagen möchten (Auszug)

"Startups sollen Kontakt zu den Großen suchen"

"Helft uns, Bedrohungen besser zu verstehen und den Transport ans Management zu erleichtern"

"Ihr müsst visibler werden - vor allem euer Vertrieb"

"Besondere Perspektive für das Tagesgeschäft des CISOs"

"Baut was, wo Sicherheit gesteigert wird und Sicherheit sichtbar wird"

→ "3 Punkt Gurt"

"Wir brauchen Produkte mit weltweiter Verfügbarkeit und hoher Performance, mit guter Qualität zum konkurrenzfähigen Preis"



Was noch?

(Ausblick auf weitere Themen der gesamten Arbeit)

- Wunsch und auf der Suche nach Produkten die fehlen
- Sicherheitsanforderungen in 5 respektive 10+ Jahren
(*Integration, Zusammenführung, Separation, Services*)
- Mögliche Konsolidierung des Angebotes
- Leistung der Behörden im Allgemeinen
- Verschlüsselung vs. Backdoors
- Open Source (Einsatz und Förderung)
- Gemeinsames Lagezentrum
- Sympathiebewertungen
- ... uvm! 😊

Danke für ihre Aufmerksamkeit!

Das haben Sie heute gelernt:

- Die Großanwender halten viel von Ihnen
- IT-Sicherheitsprodukte müssen in Zukunft maßgeschneidert und trotzdem (weltweit) breit einsetzbar sein
- Müssen dem CISO das Leben *deutlich* erleichtern
- Transparenz: Mehr Sicherheit bei gleichzeitig weniger Wahrnehmung durch die Nutzer
- Skalierbarkeit + internationale Verfügbarkeit sind das A & O

Rückfragen gerne per E-Mail an
s^obastian {at} b^orchnicki [PUNKT) de