Information Security: Mythos vs. Realität

STIHL INFORMATION SECURITY

mbuf focus day IT-Security

23.07.2019

MYTHOS 1

Ein starkes Passwort ist ausreichend, um persönliche und Firmen Daten vor unberechtigten Zugriffen zu schützen.

Realität: Passwort

- Meist genutzte Passwörter laut *National Cyber Security Center*:

1) 123456
2) 123456789
3) qwerty
4) password
5) 111111
6) 12345678
7) abc123
8) 1234567
9) password1
10) 12345
11) 1234567890
12) 123123
13) 000000
14) Iloveyou
15) 1234

Quelle: https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordTop100k.txt

Realität: Passwort

Knuddels.de

September 2018
800.000 geklaute Accounts

Comcast

Februar 2016
600.000 geklaute Accounts

8fit

Juli 2018
15 Mio. geklaute Accounts

500px

Juli 2018
14,9 Mio. geklaute Accounts

Adobe

Oktober 2013
153 Mio. geklaute Accounts

VTech

November 2015
4,8 Mio. geklaute Accounts

League of Legends

Juni 2012
340.000 geklaute Accounts

Quelle: https://haveibeenpwned.com/PwnedWebsites

Realität: Passwort

Geplante „Password Spraying“ Attacke auf STIHL

- Alle Anmeldevorgänge im Zeitraum 27. – 29.03.2019

- „Password Spraying“ Logs im Zeitraum 27. – 29.03.2019

„Password Spraying“ Attacke kann im allgemeinen Log-Aufkommen untergehen!

Realität: Passwort

2 FACTOR AUTH

Die sicherste Variante zur Absicherung eines Accounts ist die Nutzung einer 2-Faktor-Authentifizierung
(z.B. Google Authenticator)

BE DIFFERENT

Verwenden Sie unterschiedliche Passwörter für unterschiedliche Accounts

PASSWORD SAFE

Um sich viele unterschiedliche Passwörter zu “merken” eignen sich ein Passwort Safe als technisches Hilfsmittel
(STIHL intern: Password Safe)

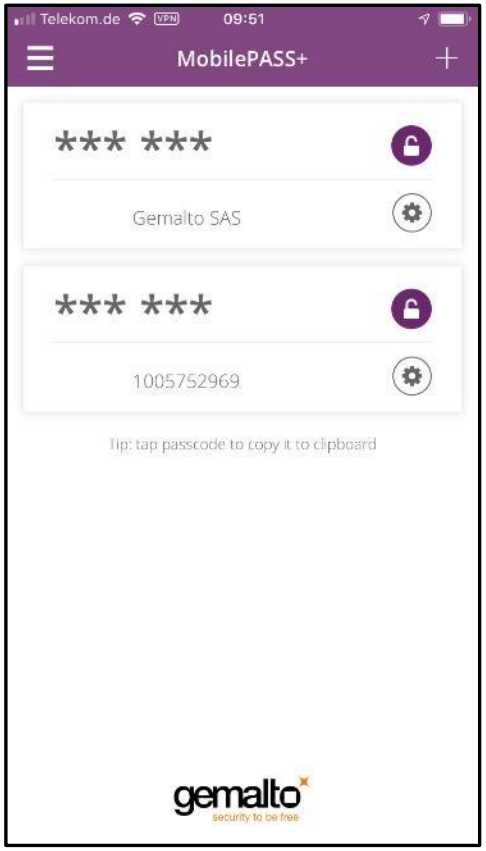
ONLY YOU

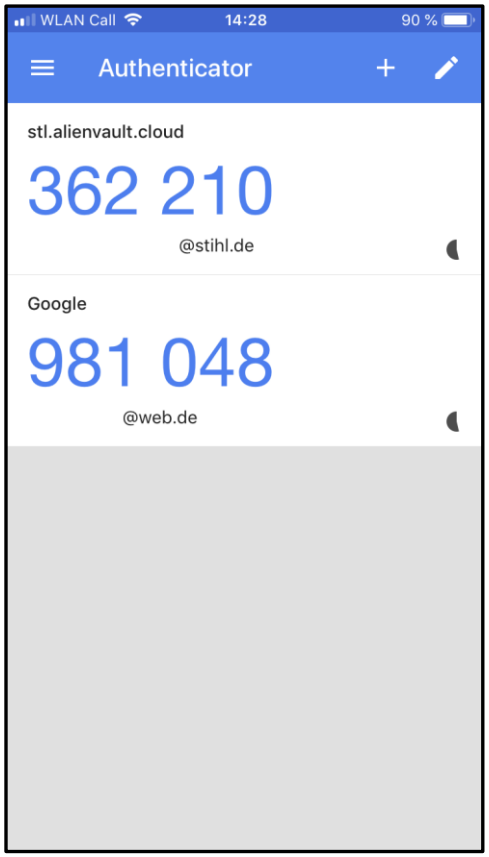
Nutzen Sie Ihre Passwörter stets nur für sich und geben Sie diese unter keinen Umständen weiter

Realität: Passwort

Beispiele für 2 Faktor Authentifizierung bei STIHL

- 2 FA Lösungen auf dem Smartphone
  - MobilePASS+ (z.B. für Home Working)
  - Google Authenticator (auch für private Anwendungen geeignet)
- Zertifikate
- Finger Print

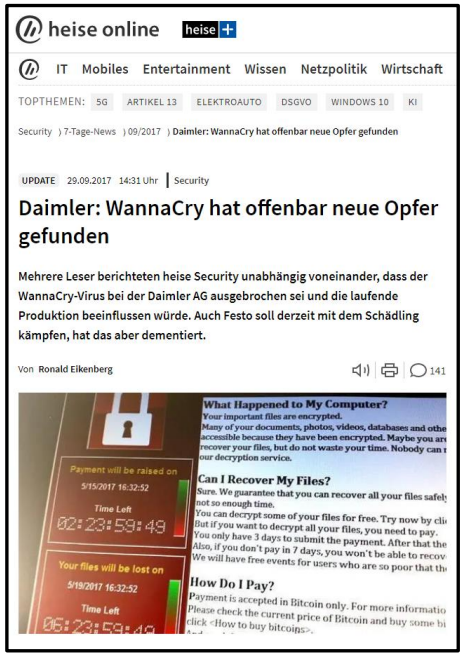




MYTHOS 2

Der Fokus von Hackern liegt ausschließlich auf großen Organisationen und börsennotierten Unternehmen.

Realität: Hackerangriffe



Quellen: https://www.thyssenkrupp.com; https://www.heise.de; https://www.wiwo.de; https://www.spiegel.de

Realität: Hackerangriffe

SPIEGEL ONLINE

WIRTSCHAFT

Maschinenbaukonzern

Cyber-Kriminelle erpressen KraussMaffei

Hacker haben den deutschen Maschinenbaukonzern KraussMaffei getroffen, die Produktion läuft nur noch eingeschränkt. Laut einem Bericht soll auch Lösegeld gefordert worden sein.

Kunststoffmaschine im Werk von KraussMaffei (Archiv)

Freitag, 07.12.2018 12:11 Uhr

Der Maschinenbaukonzern KraussMaffei ist nach eigenen Angaben von einem schweren Cyberangriff getroffen worden. Nach der Attacke vor gut zwei Wochen habe das Unternehmen mit Hauptsitz in München an einigen Standorten nur mit gedrosselter Leistung produziert, da viele Rechner aufgrund einer Trojaner-Attacke lahmgelegt worden seien, sagte ein Unternehmenssprecher.

STUTTGARTER-ZEITUNG.DE

Elektrowerkzeughersteller Metabo aus Nürtingen

Wie ein Cyberangriff das Unternehmen lähmte

Von Florian Gann - 17. Juli 2018 - 18:48 Uhr

Ein IT-Experte des Werkzeugherstellers Metabo aus Nürtingen berichtet, wie eine Cyberattacke das Unternehmen getroffen hat – und wie die Mitarbeiter damit umgegangen sind.

Ein Cyberangriff legte Metabo 2017 für mehrere Tage lahm. Foto:dpa

STUTTGARTER-ZEITUNG.DE

Baden-Württemberg

Fast 300 Hackerangriffe auf Firmen und Behörden

Von red/dpa/lsw - 04. März 2018 - 11:30 Uhr

Nicht nur die Bundesregierung, auch Institutionen in Baden-Württemberg werden Opfer von Internetkriminalität. Die Fachleute beim Landeskriminalamt sind in solchen Fällen die richtigen Ansprechpartner.

Etwa 300 Hackerangriffe hat es 2017 in Baden-Württemberg auf Firmen und Behörden gegeben. *Foto: dpa*

Stuttgart - Fast 300 Mal haben sich im vergangenen Jahr Firmen und Behörden beim Landeskriminalamt (LKA) gemeldet, um Hackerangriffe anzuzeigen. Dort gibt es eigens für diese Fälle die Zentrale Ansprechstelle Cybercrime (ZAC). Baden-Württemberg sei im Vergleich von Cyber-Attacken ebenso betroffen wie andere Bundesländer, sagte Hauptkommissar Bernhard Lacker von der ZAC. „Das IT-Sicherheitsbewusstsein ist durchaus noch ausbaufähig."

Frankfurter Allgemeine

Diginomics

F.A.Z.-INDEX DAX EUR/USD DOW JONES ALLE KURSE

BEINAHE TÄGLICHE ANGRIFFE

Hacker greifen deutschen Mittelstand an

VON BASTIAN BENRATH - AKTUALISIERT AM 08.01.2019 - 06:56

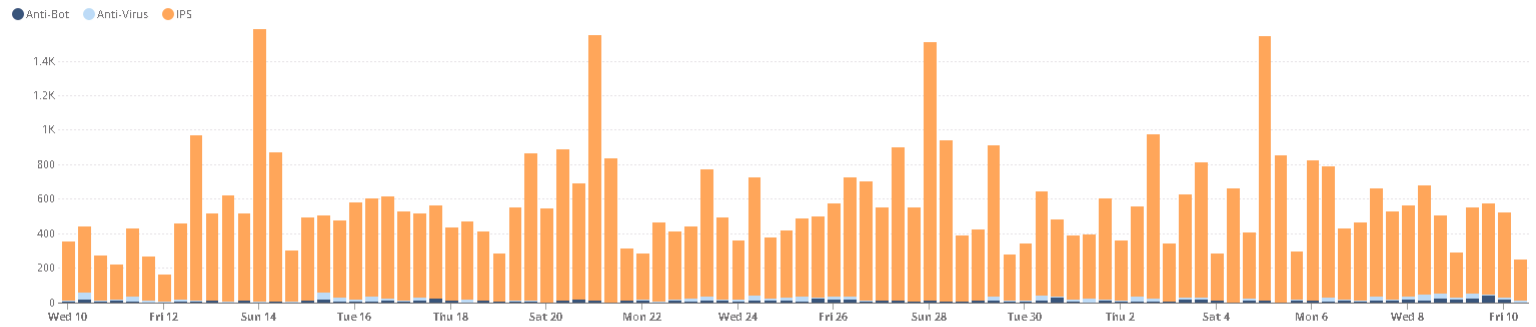
Nicht nur Politiker und Prominente sind Opfer von Hackern. Die Wirtschaft kosten Cyberkriminelle im Jahr mehr als 50 Milliarden Euro. Und doch sind einige Experten optimistisch.

Quellen: https://www.spiegel.de; https://www.stuttgarter-zeitung.de; https://www.faz.net

Realität: Hackerangriffe

Angriffalarme auf STIHL innerhalb der letzten 30 Tage

CYBER ATTACK TRENDS



NOT PREVENTED ATTACKS

0 Users received malicious mails
The number of users who attackers attempted to target using malicious mail

0 Hosts downloaded malicious files
The number of hosts which attempted to download a malicious file

0 Hosts accessed malicious websites
The number of hosts which attempted browsing to a malicious website or to web pages hosting active malicious web content such as exploit kits and crypto-mining code

6 Directly targeted hosts
The number of servers and other hosts which were attackers attempted to attack directly

13 Hosts scanned by attackers
The number of hosts which attackers attempted to scan for reconnaissance and vulnerability discovery purposes

PREVENTED ATTACKS

68 Users received malicious mails
The number of users who were targeted using malicious mail

24 Hosts downloaded malicious files
The number of hosts which downloaded a malicious file

177 Hosts accessed malicious websites
The number of hosts which browsed to a malicious website, or to web pages hosting active malicious web content such as exploit kits and crypto-mining code

311 Directly targeted hosts
The number of servers and other hosts which were directly targeted by attackers

181 Hosts scanned by attackers
The number of hosts which were scanned by attackers for reconnaissance and vulnerability discovery purposes

MYTHOS 3

Der Einsatz von Anti-Virus Software sorgt für einen ganzheitlichen Schutz meines Unternehmens.

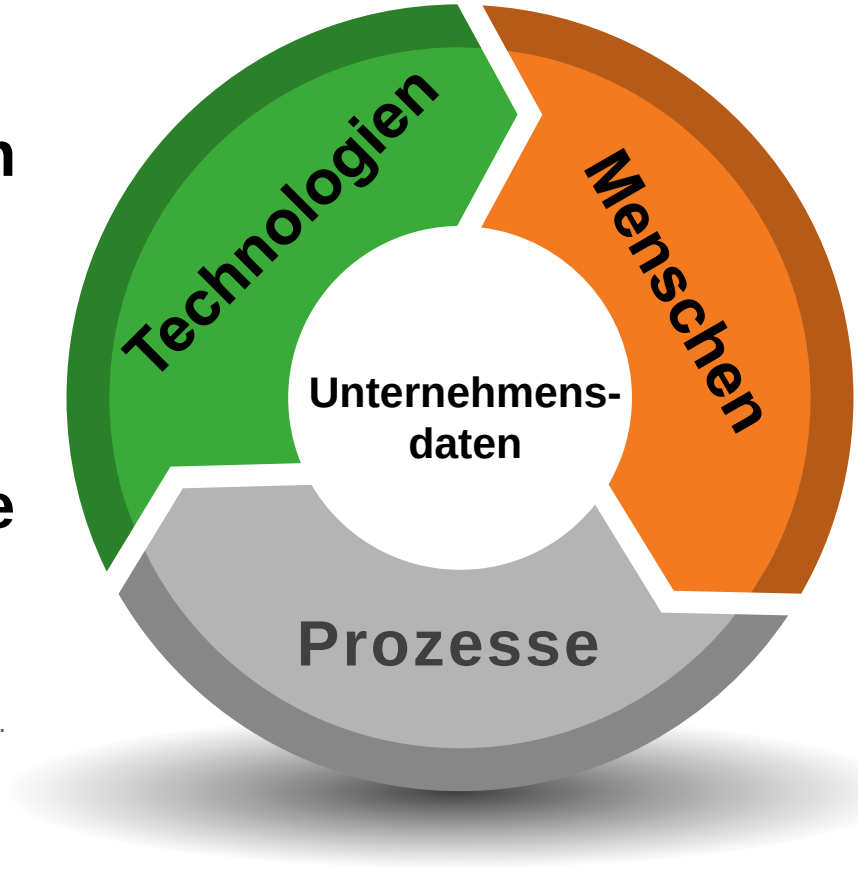
Realität: ganzheitlicher Schutz

Technologien

Anti-Virus, Anti-Malware, Firewall, Verschlüsselung, E-Mail Sicherheit, usw.

Prozesse

Informationsklassifizierung, Risikomanagement, Lieferantenüberprüfung, Incident Management, usw.

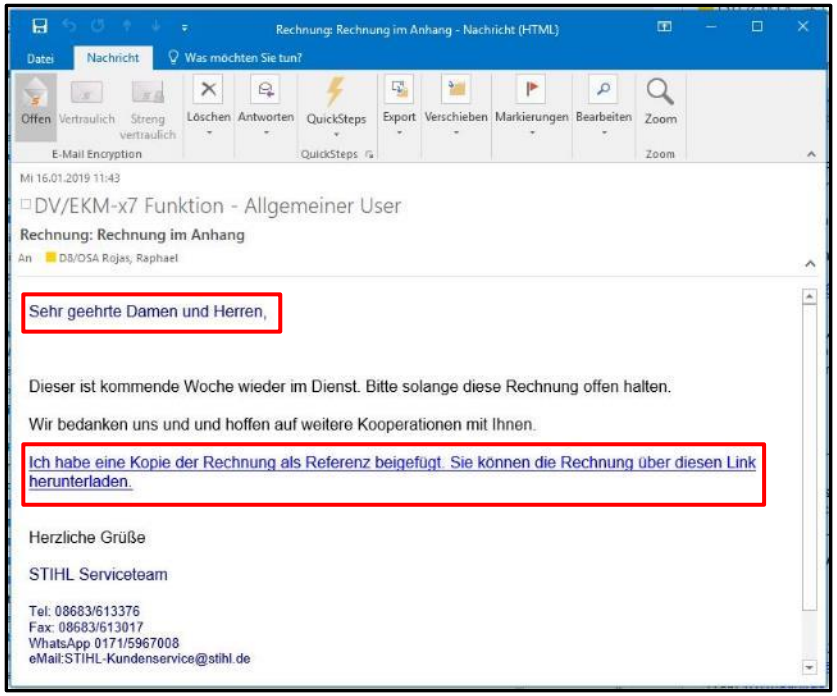


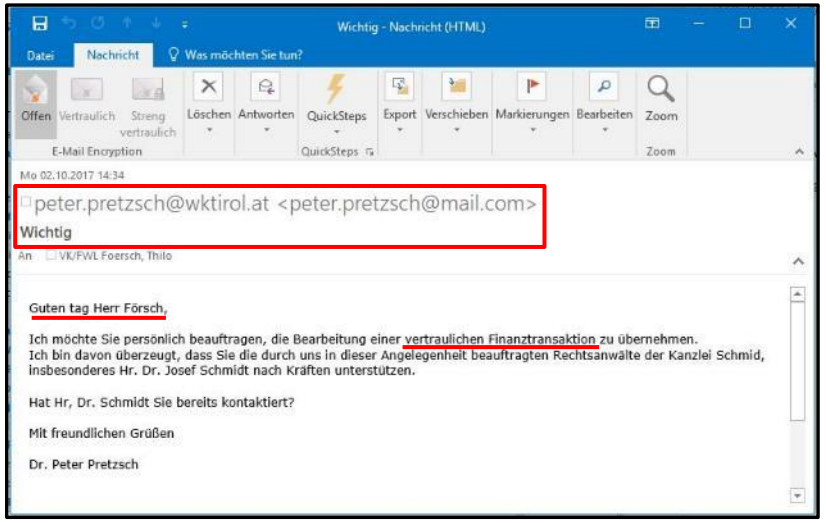
Menschen

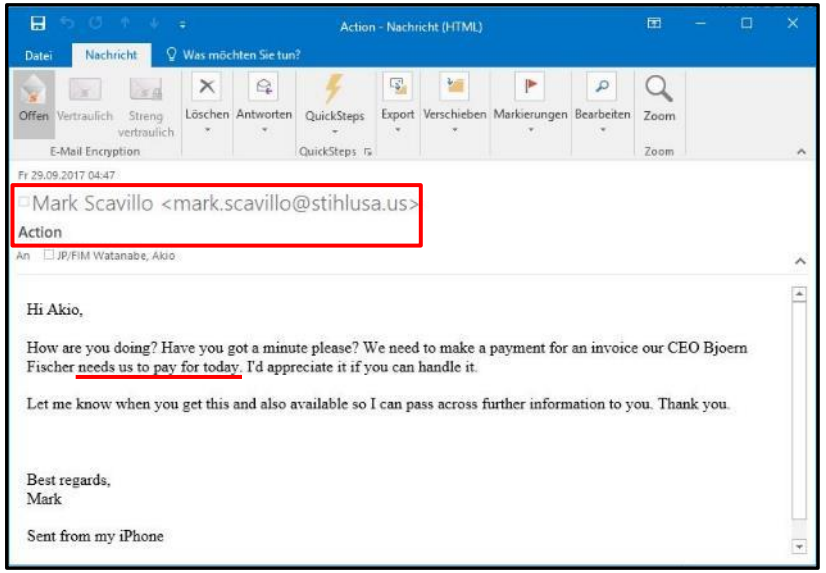
Mitarbeiter Schulungen, Mitarbeiter mit Zeit und Qualifikation für Informationssicherheit usw.

Realität: ganzheitlicher Schutz

Hätten Sie es erkannt?







MYTHOS 4

Informationssicherheits-Bedrohungen kommen ausschließlich von außerhalb des Unternehmens.

Realität: Bedrohungen von Innentätern

CIO VON IDG

Newsletter Whitepaper Jobs Shop

Events CIO-Netzwerk Benchmarks Bildung

Schutz vor Insider Threat mit DLP, UBM, SIEM und Forensik

Absichern gegen Innentäter

10.09.2018 Von Jens Dose (Redakteur)

Die Gefahr durch Datenlecks aus dem Inneren des Unternehmens darf nicht unterschätzt werden. Verschiedene Sicherheitskonzepte sollen dieses Problem lösen.

Empfehlen
Twitter
Facebook
Xing
LinkedIn
Drucken

Unternehmensdaten gegen Bedrohungen von innen abzusichern, ist ein nicht zu unterschätzender Teil der Sicherheitsstrategie. Laut dem Insider Threat Index 2018 von Data Loss Prevention (DLP)-Anbieter Clearswift, sollen in Europa die Insider-Bedrohungen zwar leicht gesunken sein aufgrund gesteigerter Sensibilität für kritische Daten und deren Schutz durch die verschärften Vorgaben der DSGVO.

Dennoch mache die direkte Bedrohung durch böswillige oder unachtsame Mitarbeiter 38 Prozent der Vorfälle aus. Im erweiterten Unternehmen (inklusive Zulieferer, Kunden und ehemalige Mitarbeiter) sollen es sogar 75 Prozent sein. Für die Studie wurden 400 IT-Entscheider aus Unternehmen mit mehr als 1.000 Mitarbeitern in Deutschland, Großbritannien und den USA befragt.

Auch in Deutschland nehmen laut der IDC-Studie "IT-Security in Deutschland 2018" uninformierte oder fahrlässige Mitarbeiter mit 37 Prozent den Spitzenplatz der Risikofaktoren innerhalb von Unternehmen ein. Das Gefahrenpotential durch vorsätzliches Fehlverhalten oder Datenmissbrauch wird von 28 Prozent der 230 befragten Organisationen in Deutschland mit mehr als 20 Mitarbeitern als Security-Risiko bezeichnet.

Schwarze Schafe unter den Mitarbeitern sind eine ernstzunehmende Bedrohung für die Sicherheit der Unternehmensdaten.

KREISZEITUNG Böblinger Bote

NACHRICHTEN SPORT THEMENWELT GEMEINDEBLÄTTER WAS-WANN-WO SERVICE AKTIONEN ABO Artikelsuche ...

Herrenberger Hacker wandert hinter Gitter

Böblinger Amtsgericht verurteilt 26-jährigen zu drei Jahren und drei Monaten - Haftbefehl wegen Fluchtgefahr umgehend vollstreckt

Feedback

Wegen besonders schwerer Computersabotage hat das Böblinger Amtsgericht einen 26-jährigen Hacker aus Rottenburg zu drei Jahren und drei Monaten Haft verurteilt. Er hatte einen Cyberangriff auf den Herrenberger Standort der "United Digital Group" gestartet.

Quellen: https://www.cio.de, https://www.krzbb.de

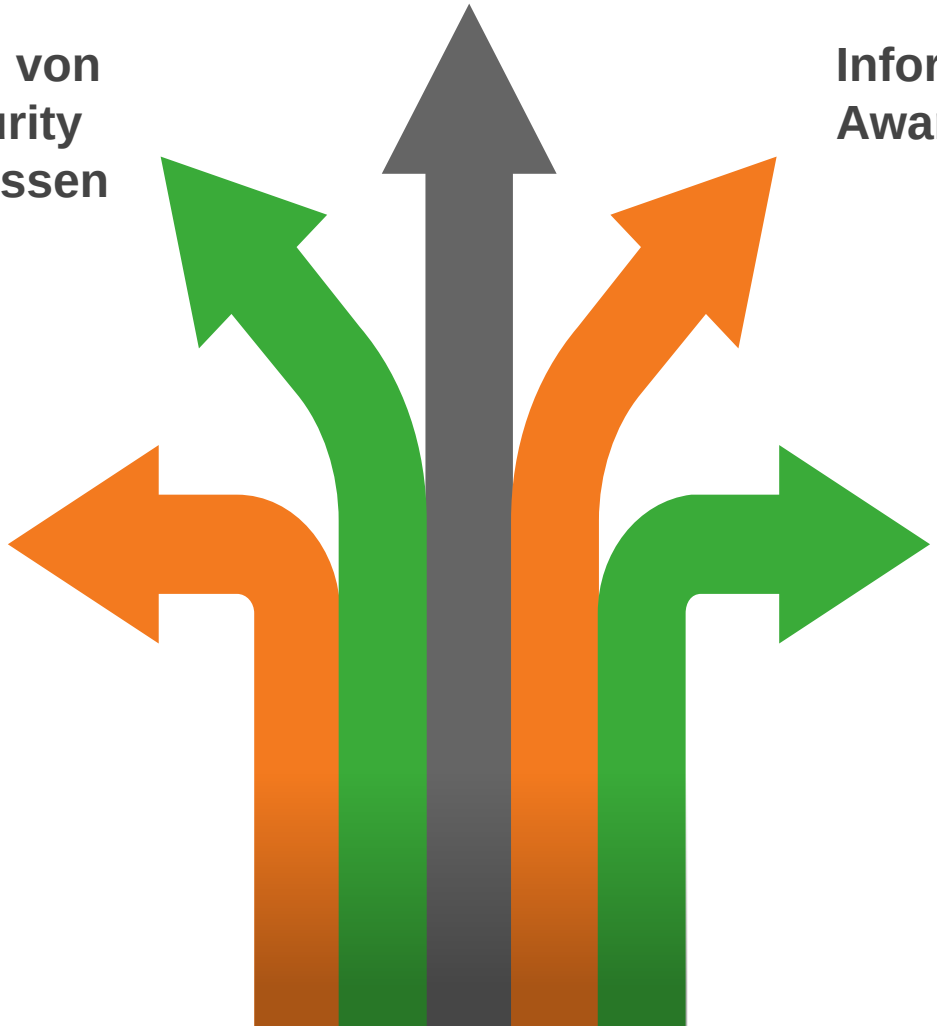
STIHL Information Security

Aktuelle Vorhaben

Implementierung eines globalen Security Operations Center (SOC)

Implementierung von Information Security relevanten Prozessen und Richtlinien

Information Security Awareness Schulungen

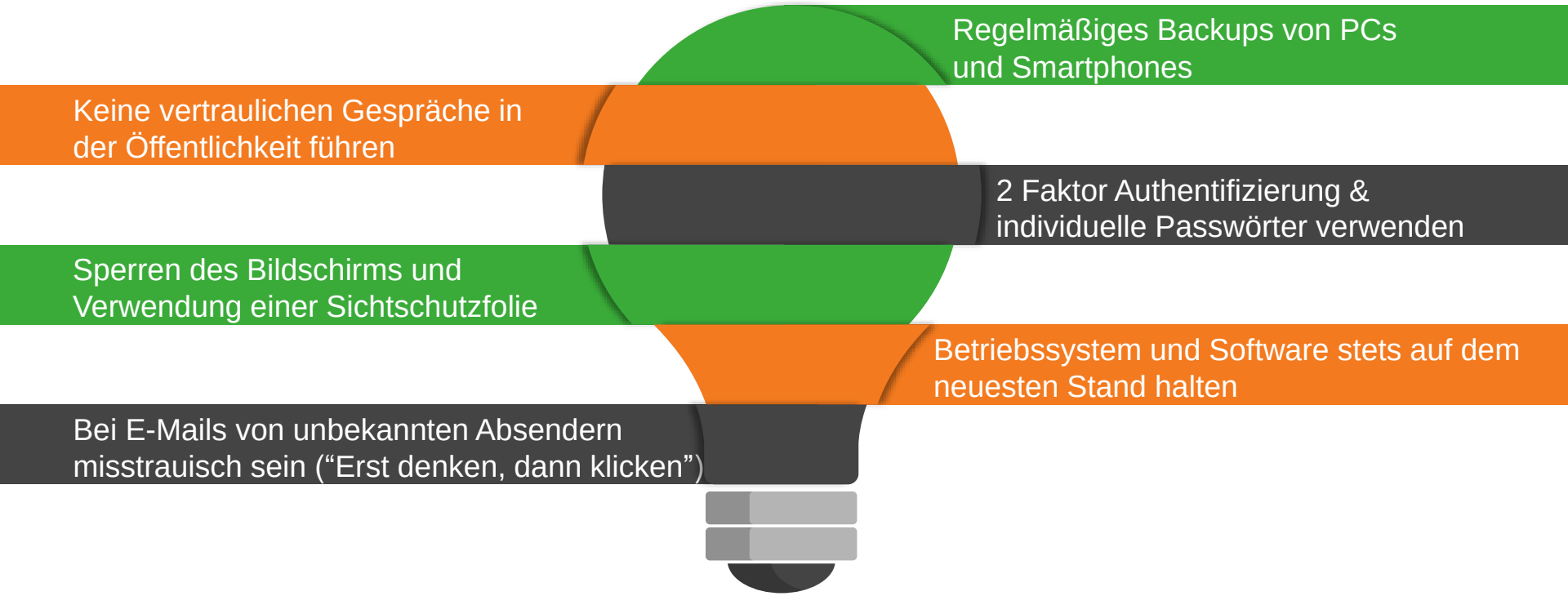


Koordination von Penetrationstests

„Information Security Audits for Suppliers“ (ISA4S)

STIHL Information Security

1 x 1 zum Schutz von beruflichen und private Daten



Don‘t do it like this ;-)

Quellen: https://www.linkedin.com/company/the-cyber-security-hub/