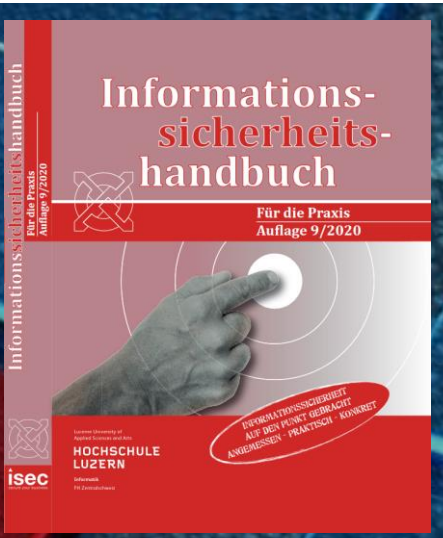
Cyber-Security für Unternehmer & Private

SIDLER Information Security

FabLab Zug - Wissen & Essen – 6. Dezember 2022

Cyber-Angriff und Verteidigung

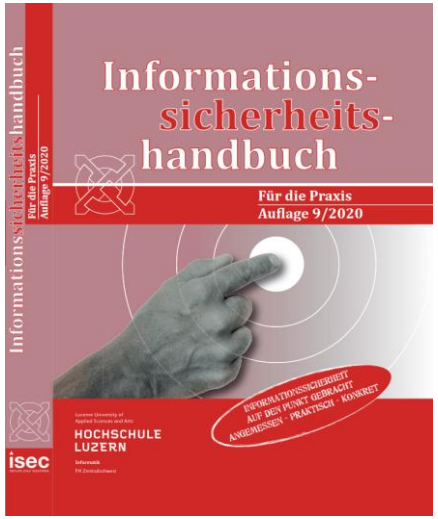
FAB LAB ZUG



Mitautor
IT-Sicherheitshandbuch für die Praxis
ISBN: 3-9521208-3-9 www.sihb.ch

Wolfgang Sidler
Inhaber SIDLER Information Security GmbH
Datenschutz- (DPO) und Security-Officer (CISO)
www.sidler-security.ch

Wolfgang Sidler - Security Berater & CEO



Mitautor
IT-Sicherheitshandbuch für die Praxis
ISBN: 3-9521208-3-9 www.sihb.ch

- Wirtschaftsinformatiker, Master of Advanced Studies HSLU in **Information Security** und Certificate of Advanced Studies HSLU in **Blockchain**
- **22 Jahre** Informationssicherheits-Erfahrung
- **10 Jahre** Stv. Datenschutzbeauftragter des Kantons Luzern von 2009 - 2018
- **6 Jahre** IT-Security Officer bei der Privatbank Julius Bär in Zürich und New York
- **3 Jahre** internationale Security-Beratung (USA und Oman)
- **7 Jahre als CISO und DPO als Mandat bei Kunden**

Kontakt
www.sidler-security.ch
wolfgang.sidler@sidler-security.ch

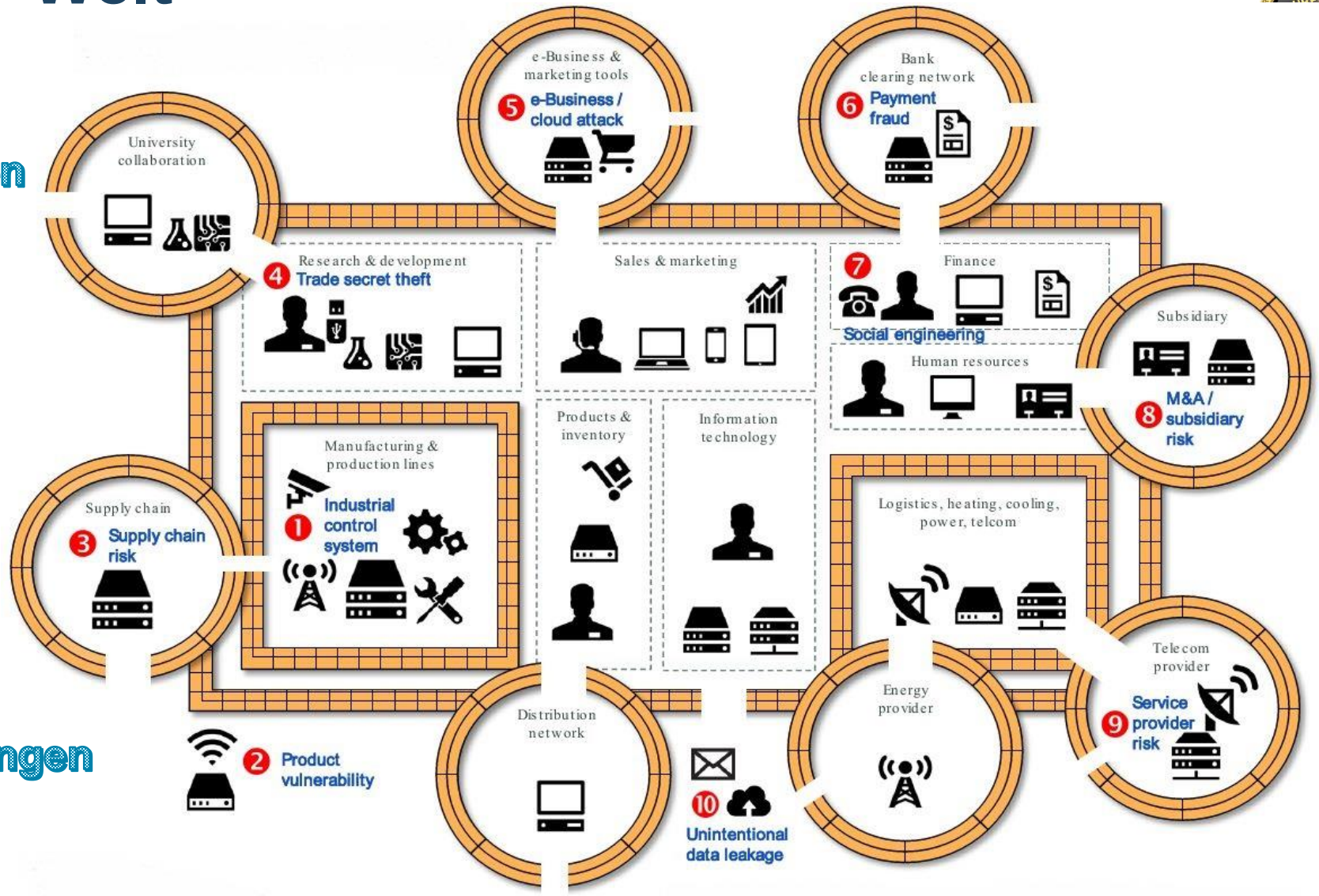
Wirtschaftsschutz-Schweiz
Director IT-Security Services & Founding Partner
Swiss Business Protection AG
www.swissbp.ch

Video als Einstieg in die Cyber-Security

Die “alte” IT-Welt

Die “neue” IT-Welt

- Vertragliche Anforderungen
- Neue Schwachstellen
- Mobilität
- neue Produkte
- Abhängigkeiten
- Cloud-Services
- Komplexität
- höhere Kunden-Anforderungen



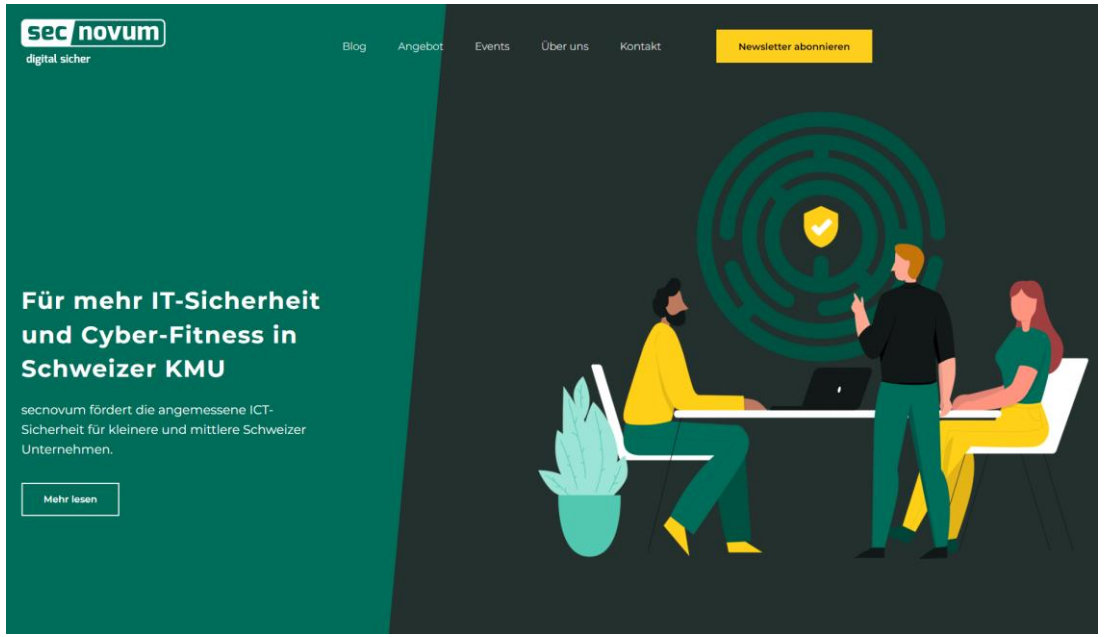
Aktuelle Cyber-Attacken und Top-Bedrohungen

SIDLER Information Security

ÜBER 10 JAHRE FÜR SIE DA

Top 3 Bedrohungen für die IT-Sicherheit bei KMU

1. Malware / Schadsoftware
2. Identitätsdiebstahl
3. Unvorbereitet auf Krisen



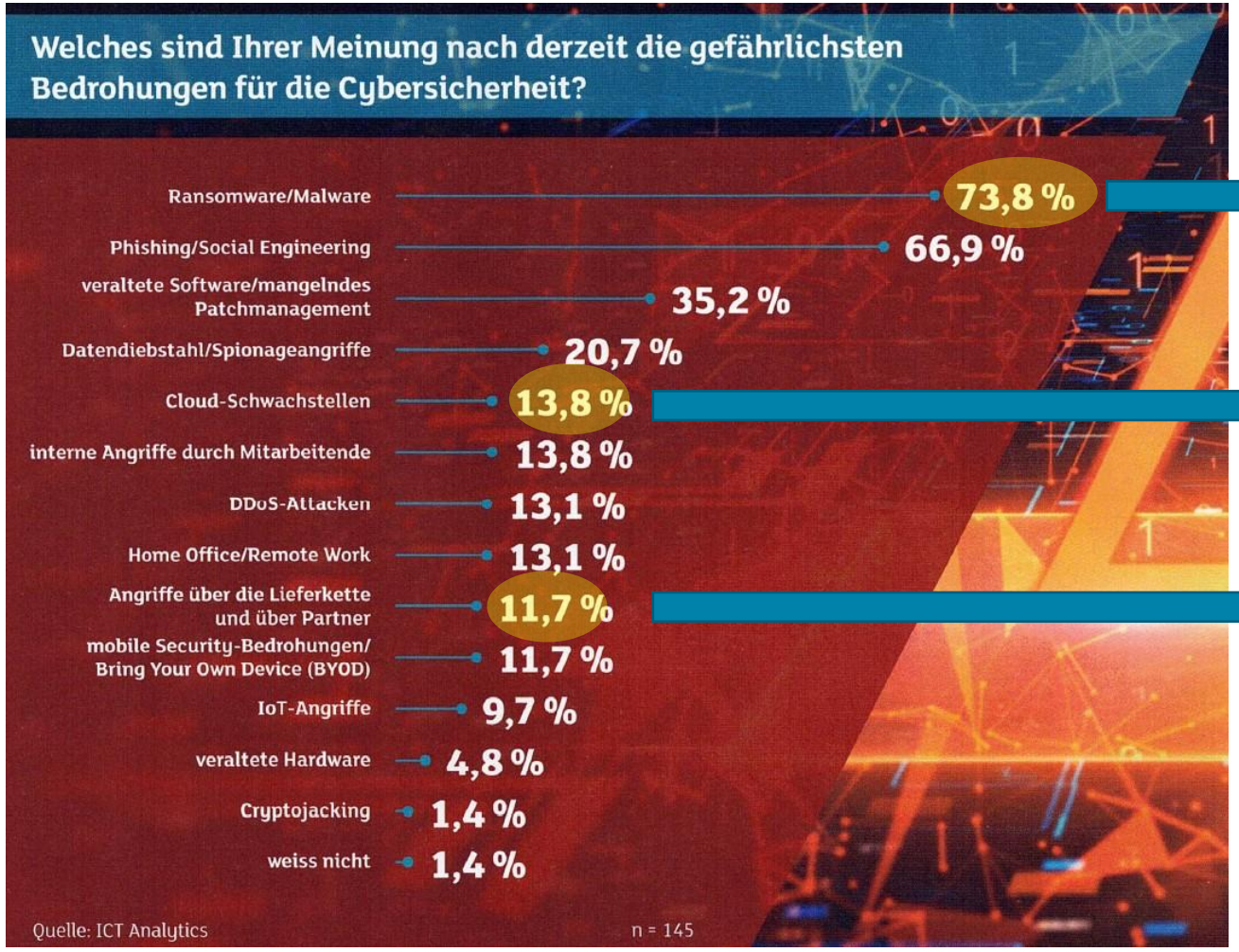
Quelle:

sec novum digital sicher

https://www.secnovum.ch

FAB LAB ZUG

Aktuelle CH-Studie – Cyber-Security Bedrohungen



Vermehrte Ransomware-Angriffe

Sollte m.E. höher liegen, denn nicht alle Cloud-Lösungen sind sicher – hier ist zwingend ein Cloud Risk-Assessment nötig !

Das Lieferanten-Management wird meistens unterschätzt. Fehlende NDAs, Weisungen oder Zertifizierungen.

Aktuelle Cyber-Attacken

«Global Digital Trust Insights Survey» von PwC *01.11.2022, 08:43 Uhr*

Schweizer Firmen erwarten 2023 wesentlich mehr Ransomware-Attacken

Schweizer Firmen sind sich der Gefahr durch Ransomware-Angriffe bewusst. Ja, eine Mehrheit von ihnen erwartet sogar, dass diese Attacken 2023 nochmals wesentlich zunehmen werden. Dies ist eines der Ergebnisse der aktuellen «Global Digital Trust Insights Survey» von PwC.

Eine Mehrheit der Unternehmen in der Schweiz, konkret 51 Prozent von ihnen, erwartet im nächsten Jahr wesentlich mehr Ransomware-Angriffe. Das sind doch um einiges mehr als global. Nur 32 Prozent der weltweiten Firmen gehen von einer entsprechenden Zunahme aus. Dies ist eines der Ergebnisse der PwC-Umfrage «Global Digital Trust Insights Survey», bei der mehr als 3500 Führungskräfte aus 65 Ländern befragt wurden, darunter deren 70 aus der Schweiz.

Doch nicht nur bei Ransomware-Angriffen erwartet ein höherer Prozentsatz der befragten Schweizer Unternehmen 2023 eine Steigerung der Vorkommnisse gegenüber dem weltweiten Durchschnitt. Dies trifft bei zahlreichen erwarteten Cybervorfällen vor (vgl. Grafik).

Cyber Risk Index von Trend Micro *22.11.2022, 13:24 Uhr*

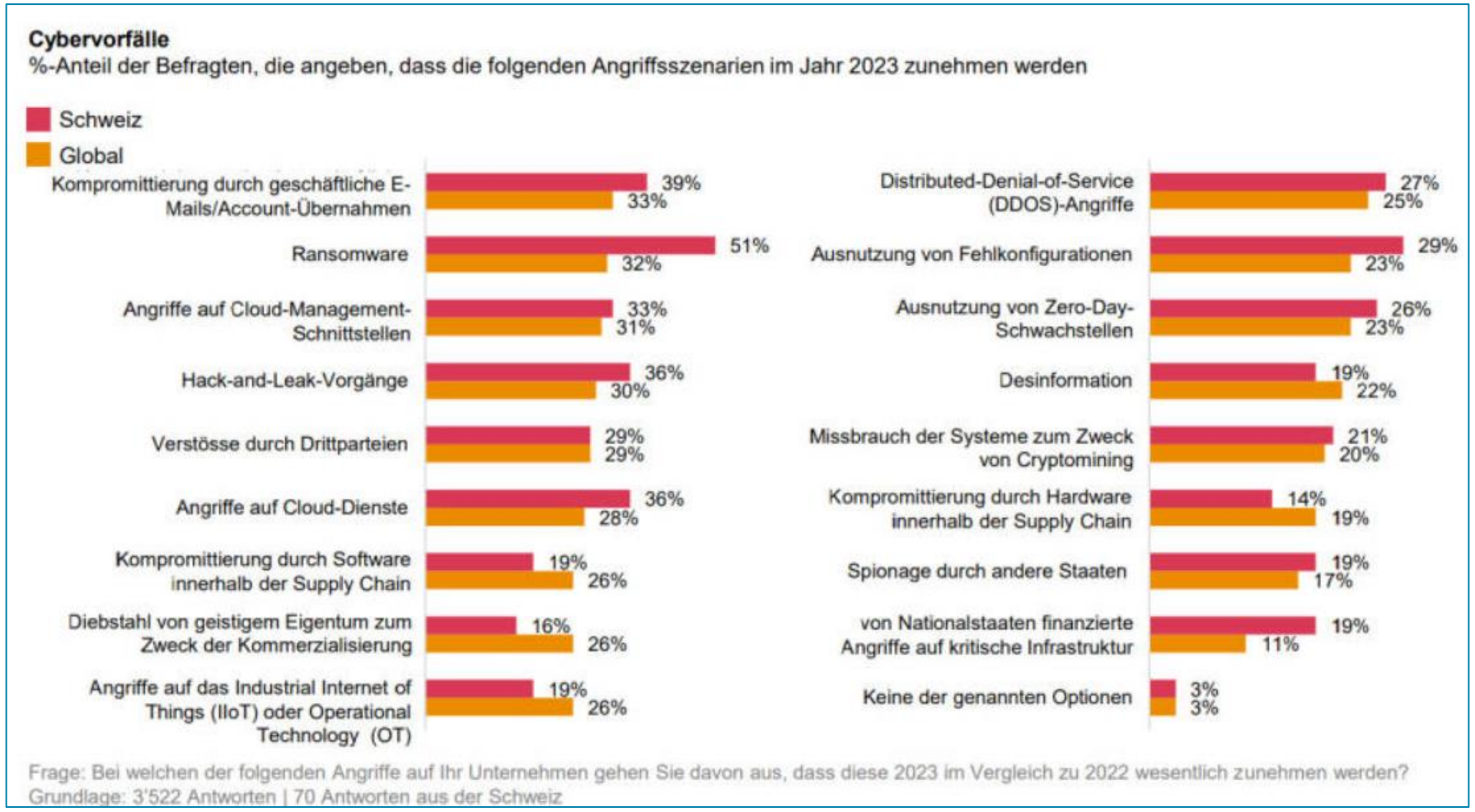
88 Prozent der Schweizer Firmen Opfer eines Cyberangriffs

In einer Studie von Trend Micro geben 88 Prozent aller in der Schweiz befragten Firmen an, in den letzten zwölf Monaten Sicherheitsvorfälle erlebt zu haben, in deren Folge Kundendaten verloren oder gestohlen wurden.

Im ersten Halbjahr 2022 erhöhte sich das Risikoniveau von -0,04 auf -0,15. Die Befragten nehmen somit ein höheres Risiko bei der Vorbereitung auf Cyberangriffe sowie in der aktuellen Bedrohungslandschaft wahr.
(Quelle: Trend Micro)

Kaum eine Firma in der Schweiz ist davor gefeit, von Hackern angegriffen zu werden. Dies zeigt der Cyber Risk Index (CRI) für das erste Halbjahr 2022 von Trend Micro. Denn darin geben 88 Prozent aller in der Schweiz befragten Unternehmen an, in den letzten zwölf Monaten Sicherheitsvorfälle erlebt zu haben, in deren Folge Kundendaten verloren oder gestohlen wurden.

Aktuelle Cyber-Attacken



Aktuelle Cyber-Attacken

21.11.2022 - 12:44 Uhr

Schweizer Admins schlafen - 2800 Server warten auf Sicherheitsupdate

Das Nationale Zentrum für Cybersicherheit (NCSC) erlebt wohl ein gewisses Déjà-vu. Das Kompetenzzentrum fordert derzeit die Betreiber von Microsoft-Exchange-Servern auf, ihre Systeme zu patchen.

Konkret geht es um die Schwachstelle "ProxyNotShell". Diese ist seit September 2022 bekannt und wird bereits aktiv von Cyberkriminellen ausgenutzt. Am 8. November veröffentlichte Microsoft einen Patch, der die Sicherheitslücke schliesst.

Und trotzdem: Zwei Wochen nach der Veröffentlichung des Patches gibt es gemäss dem NCSC noch immer 2800 über das Internet erreichbare Server, die weiterhin verwundbar sind. Angreifern wäre es also möglich, "ProxyNotShell" auszunutzen, beliebigen Code aus der Ferne auszuführen und die Server zu kompromittieren. Die Betreiber riskieren also Ransomware-Attacken, einen Datendiebstahl oder vergleichbare Cyberangriffe.

Erinnerungen werden wach

Die aktuelle Lage erinnert an die Situation im Frühjahr 2021. Damals hatte Microsoft ebenfalls ein Sicherheitsupdate für seine Exchange-Server veröffentlicht. Die damit adressierte Schwachstelle war laut dem NCSC von einem ähnlichen Ausmass wie die aktuelle Sicherheitslücke.

Das NCSC informierte daraufhin betroffene Unternehmen per Einschreiben darüber. In manchen Fällen mehrmals: Im März dieses Jahres kontaktierte das NCSC erneut 130 Schweizer Unternehmen, um sie über die Sicherheitslücke zu informieren. Und trotzdem: Mindestens ein Unternehmen reagierte nicht auf die Warnungen und wurde anschliessend Opfer einer Ransomware, wie das NCSC im April schilderte.

Aktuelle Cyber-Attacken

GovCERT.ch
@GovCERT_CH · Folgen

Wir haben heute über 130 Organisationen in der Schweiz per Einschreiben ✉️ über verwundbare MS Exchange Server informiert, darunter auch mehrere Gemeinden 🚨 Obwohl die entsprechenden Patches bereits seit Monaten zur Verfügung stehen, wurden diese bislang nicht eingespielt ⚠️

9:03 nachm. · 15. Feb. 2022

217 Antworten Teilen

12 Antworten lesen

Aktuelle Cyber-Attacken

Rohstoff für neue Phishing Attacken !

SIDLER Information Security

ÜBER 10 JAHRE FÜR SIE DA

Auch Schweizer Nummern betroffen

Hacker verscherbeln Daten von 500 Millionen Whatsapp-Usern

Fr 25.11.2022 - 12:01 Uhr
von Maximilian Schenner und tme

Auf einem Hacker-Forum stehen fast 500 Millionen vermeintliche Nutzerdaten von Whatsapp-Usern zum Verkauf. Darunter sind auch knapp 1,5 Millionen Nummern aus der Schweiz. Ob die eigene Nummer betroffen ist, lässt sich aktuell nicht klären.

Switzerland	1,592,039

Someone is allegedly selling up-to-date mobile phone numbers of nearly 500 million WhatsApp users. A data sample investigated by Cybernews likely confirms this to be true.

On November 16, an actor posted an ad on a well-known hacking community forum, claiming they were selling a 2022 database of 487 million WhatsApp user mobile numbers.

The dataset allegedly contains WhatsApp user data from 84 countries. Threat actor claims there are over 32 million US user records included.

Another huge chunk of phone numbers belongs to the citizens of Egypt (45 million), Italy (35 million), Saudi Arabia (29 million), France (20 million), and Turkey (20 million).

The dataset for sale also allegedly has nearly 10 million Russian and over 11 million UK citizens' phone numbers.

The threat actor told Cybernews they were selling the US dataset for $7,000, the UK – $2,500, and Germany – $2,000.

Such information is mostly used by attackers for smishing and vishing attacks, so we recommend users to remain wary of any calls from unknown numbers, unsolicited calls and messages.

FAB LAB ZUG

Aktuelle Cyber-Attacken

Media-Markt-Erpresser ergaunern mit Hive-Ransomware 100 Millionen US-Dollar

Das FBI hat Details zu Attacken durch den Verschlüsselungstrojaner Hive zusammengetragen. Außerdem geben sie wichtige Sicherheitstipps.

Lesezeit: 2 Min. In Pocket speichern 342

(Bild: Foxeel,Shutterstock.com)

UPDATE 18.11.2022 12:23 Uhr | Security

Die Hive-Ransomware operiert weltweit und hat hierzulande vor rund einem Jahr etwa bei der Handelskette Media Markt zugeschlagen. Die Straftäter nehmen aber auch medizinische Einrichtungen und kritische Infrastruktur ins Visier. Bei einer Ransomware-Attacke verschlüsselt ein Trojaner Daten und die Täter verlangen für Schlüssel Lösegeld. In diesem Fall sollen sie 50 Millionen US-Dollar gefordert haben. Ob das Lösegeld bezahlt wurde, ist bislang nicht bekannt.

Verschlüsselungstrojaner sind nach wie vor die Cashcow der Malwareszene. Allein im ersten Halbjahr 2021 sollen allein in den USA 590 Millionen US-Dollar erpresst worden sein. Dabei gehen die Kriminellen extrem professionell vor und nehmen Unternehmen gezielt in die Mangel.

Die Hive-Ransomware hat den Drahtziehern dem FBI zufolge bislang 100 Millionen US-Dollar in die Kassen gespült. Dafür sollen sie weltweit mehr als 1300 Firmen erpresst haben. Die Gruppe um den Erpressungstrojaner tauchte Mitte 2021 auf der Bildfläche auf.

Um Systeme zu kompromittieren, sollen die Angreifer unter anderem Sicherheitslücken in Microsoft Exchange Server ausgenutzt haben. Sie sollen aber auch versuchen, über RDP- oder VPN-Verbindungen auf Computer zu gelangen, führt das FBI aus.

Im Anschluss sollen sie unter anderem Backup- und Virenschutz-Software deaktivieren und Daten exfiltieren. Um den Druck auf Opfer zu erhöhen, drohen sie mit einer **Veröffentlichung der Daten**. Ausserdem sollen sie noch weitere Malware auf Systemen hinterlassen.

Erpressung vor einer Cyber-Attacke

```
From: Armada Collective
Subject: DDOS ATTACK!!!
Date: Wed, 9 Mar 2016 XX:XX:XX +0000

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE
DECISION!

We are Armada Collective.
http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-
hosting-providers

All your servers will be DDoS-ed starting Monday (March 14) if you
don't pay protection - 25 Bitcoins @
17j7onEtLgS2pd6qLekKQCteqTrnAFXZVS
If you don't pay by Monday, attack will start, price to stop will
increase to 50 BTC and will go up 20 BTC for every day of attack.

This is not a joke.
Our attacks are extremely powerful - sometimes over 1 Tbps per second.
So, no cheap protection will help.

Prevent it all with just 25 BTC @ 17j7onEtLgS2pd6qLekKQCteqTrnAFXZVS
```

Umgang mit Passwörter – bedenklich !?

Untersuchung von Nordpass

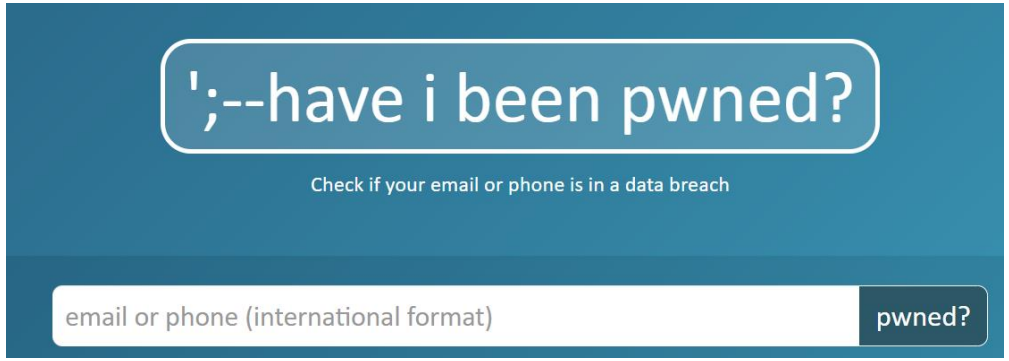
Echt jetzt? "Password" ist das beliebteste Passwort in diesem Jahr

Mo 28.11.2022 - 12:06 Uhr
von Coen Kaat und tme

Dieses Jahr hat es ein neues Passwort auf die Liste der meistgenutzten Passwörter geschafft: "Password" löste "123456" ab. Die restlichen Einträge der Liste zeigen ebenfalls, dass die Passworthygiene noch immer einiges zu wünschen übrig lässt.

Es ist wieder einmal so weit: Nordpass zeigt der Welt auf, wie unnütz ein Passwortschutz zuweilen ist. Der britische Anbieter von Passwortmanagern stellt jährlich eine Liste der häufigsten Passwörter zusammen. Die aktuelle Liste ist - wie jedes Jahr - voller Alibi-Passwörter wie "password", "123456", "qwerty" und Co.

Wieso Alibi-Passwörter? Weil diese Passwörter nur eingetippt werden, um einen Passwortzwang zufrieden zu stellen. Den Schutz erhöhen sie nicht. Mit wenigen Ausnahmen lassen sich alle 200 gelisteten Kennwörter in wenigen Sekunden mit Cracking-Tools knacken.



https://haveibeenpwned.com

Erkenntnisse

Deutschland

Hol dir die Passwortliste von 2019-2021

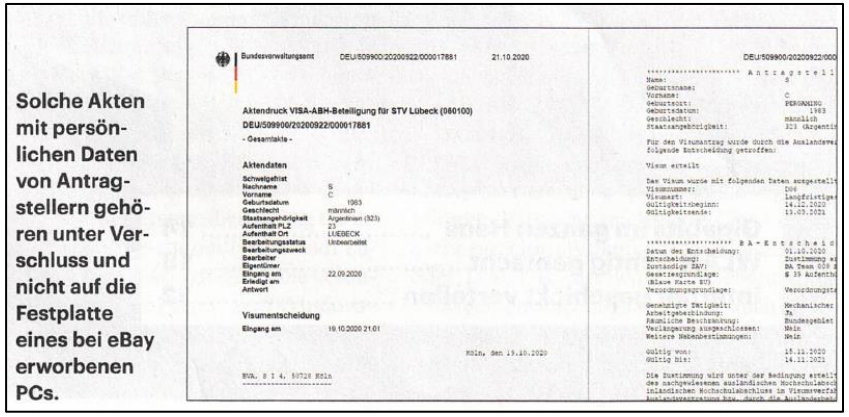
RANG	PASSWORT	BENÖTIGTE ZEIT ZUM PASSWORT-KNACKEN	ANZAHL
1	123456	< 1 Sekunde	10.359
2	password	< 1 Sekunde	2.901
3	123456789	< 1 Sekunde	2.669
4	12345	< 1 Sekunde	2.396
5	hallo	< 1 Sekunde	1.993
6	passwort	< 1 Sekunde	1.918

https://nordpass.com/de/most-common-passwords-list/

Nicht wissen oder einfach naiv !?

Datenschutz unbedacht

Festplatte mit über 33.000 hochsensiblen Mails aus dem Ausländeramt Lübeck bei eBay verkauft



Solche Akten mit persönlichen Daten von Antragstellern gehören unter Verschluss und nicht auf die Festplatte eines bei eBay erworbenen PCs.

Heikle Daten

Erotik, Kontonummern und Steuererklärung auf Occasion-Laptops

Wer seinen Laptop verkaufen will, muss aufpassen: Mit geringem Aufwand lassen sich höchst private Daten wieder herstellen.

Christof Schneider
Dienstag, 22.11.2022, 20:46 Uhr

https://www.srf.ch/sendungen/kassensturz-espresso/kassensturz/heikle-daten-erotik-kontonummern-und-steuererklaerung-auf-occasion-laptops

Menschliches Fehlverhalten

Innert **6 Monaten** verloren gegangene mobile Geräte in London:

2001
- 62‘000 Handys (3 pro Taxi)
- 2’900 Notebooks
- 1‘300 PDAs

2004
- 63‘135 Handys
- 4‘973 Notebooks
- 5‘838 PDAs

2006
- 54‘872 Handys
- 3‘179 Notebooks
- 4‘718 PDAs
- 923 Memory Sticks

Fundsachen 07. Januar 2014 08:06; *Akt: 07.01.2014 10:19*

Pendler haben 12'000 Handys im Zug vergessen

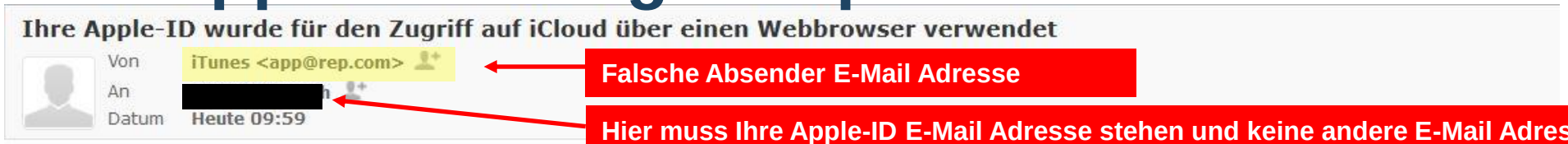
100'000 Gegenstände haben Schweizer 2013 in Zügen und Bahnhöfen liegen lassen – vom Rollstuhl über Sexspielzeug bis zur Urne. Nur wenig mehr als die Hälfte davon holten sie ab.

Ein Metalldetektor, eine Urne, ein Rollstuhl und eine Beinprothese: Roland Widmer von Fundsachenverkauf.ch mit einigen der Fundgegenstände aus dem Jahr 2013.

Bild: hal

Taschen, Koffer, Kleider und Elektrogeräte: Im Keller des Fundsachenverkauf.ch in Zürich stapelt sich die Ware auf Holzpaletten und in Kisten mit Aufschriften wie «Spielzeug», «Schmuck», «iPhone» oder «Erotik». Hier landet, was in der Schweiz in Zügen und Postautos sowie an Bahnhöfen und Flughäfen liegen geblieben ist und nicht abgeholt wurde.

Apple Phishing Beispiel



Falsche Absender E-Mail Adresse

Hier muss Ihre Apple-ID E-Mail Adresse stehen und keine andere E-Mail Adresse!

Dieses E-Mail erschreckt Sie als Benutzer einer Apple-ID

Hallo,

Ihre Apple-ID wurde für utilizzatoden Zugriffauf iCloud über einen Webbrowser verwendet.

Datum und Uhrzeit: **23 Oktober 2019, 09:39 PDT**

IP-Adresse, Ort: **180.166.56.65, China - Shanghai**

Wenn Sie sich kürzlich bei iCloud angemeldet haben, können Sie diese E-Mail ignorieren.

Wenn Sie diese änderungen nicht vorgenommen haben oder der meinung sind, dass eine unbefugte Person auf Ihren Account zugegriffen hat, klicken Sie auf die Meine Apple ID.

Mit freundlichen Grüßen,

Apple Support

IDApple | Supporto | Normesullaprivacy
Copyright © 2019
Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland.
Alle Rechte vorbehalten.

Was ist hier falsch?

- E-Mail an falsche E-Mail Adresse
- Absender «komisch»
- Text-Inhalt «utilizzatoden»???
- Schreibfehler im Text
- Komischer Footer

Apple Phishing Beispiel

Tipp

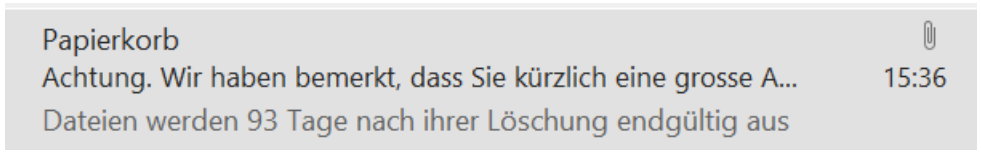
Immer die URL-Adresse und den Deutschen-Text überprüfen. Apple ist per «Du» und die Phishing-Seite per «Sie».

Lassen Sie sich nicht täuschen und passen Sie auf!

Fingierte Phishing Attacke

Mit einer fingierten Phishing Attacke können wir die Wirksamkeit unserer Sicherheits-Massnahmen und –Sensibilisierung prüfen.

Outlook E-Mail Eingang



Geänderte URL: z.B. statt fantastik.ch → fantastlk.ch

Achtung: WebCam aktiv!

Bund empfiehlt das Abkleben von Webcams
Das Nationale Zentrum für Cybersicherheit (ex. Melani) des Bundes empfiehlt, alle Webcams temporär abzukleben. Dadurch schütze man sich vor unerwünschten Zuschauern.

Tausende von Webcam-Besitzer fielen einem Hackerangriff zum Opfer. Darunter befanden sich nach neusten Erkenntnissen auch **383 Webcams aus der Schweiz**.

Watch Panasonic camera in
Switzerland
Zurich

Country:	Switzerland. You can see other **online cameras** in Switzerland.
Country code:	CH
Region:	Zurich
City:	Zurich. **View CCTV online** in Zurich.
Latitude:	47.366670
Longitude:	8.550000
ZIP:	8045
Timezone:	+02:00
Channels:	1
Manufacturer:	Panasonic

Tipp:
Default Passwort ändern!

WebCams im Internet ohne Passwort!

Auf einer öffentlichen Webseite haben Hacker über 3‘000 WebCams von der ganzen Welt ohne Schutz aufgeschaltet. **Alle WebCams hatten kein Passwort – Kein Hack! (22. Feb. 2017 – 11:15)**

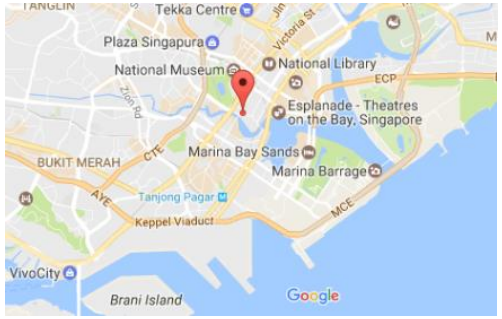
St. Petersburg

Ukraine

China

Singapore

Welcome | **Most popular** | Manufacturers | Countries | Places | Cities | Timezones | New online cameras | FAQ | Contacts



Country: Singapore. You can see other **online cameras** in Singapore.
Country code: SG
Region: Singapore
City: Singapore. **View CCTV online** in Singapore.
Latitude: 1.289670
Longitude: 103.850070
ZIP: 148943
Timezone: +08:00
Manufacturer: Panasonic

In der Schweiz 383 Cams!

Tipp:
Default Passwort ändern!

Mini-Spione und GSM Mini-Sender

Preis CHF 170.-

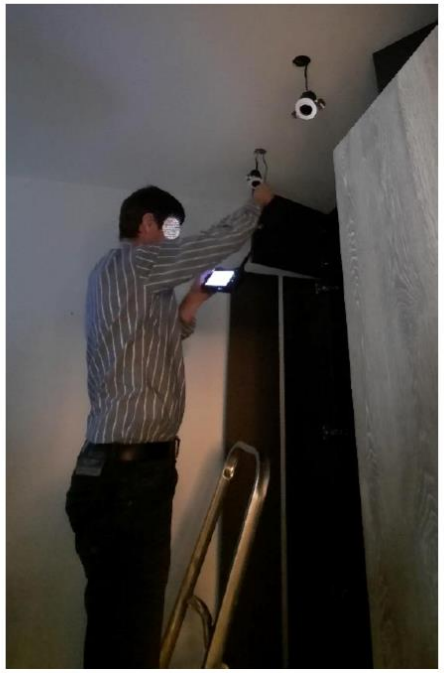
Der Akku versorgt den Mini-Sender bis zu **einer Woche lang im Standby** mit Strom. Eine dauerhafte Übertragung des Signals kann bis zu 2 Stunden lang erfolgen. Rufen Sie den GSM Sender an und hören Sie in das Umfeld hinein. Auch können Sie eine SMS an den Sender senden, nach deren Empfang der Audiosender Sie zurückruft.

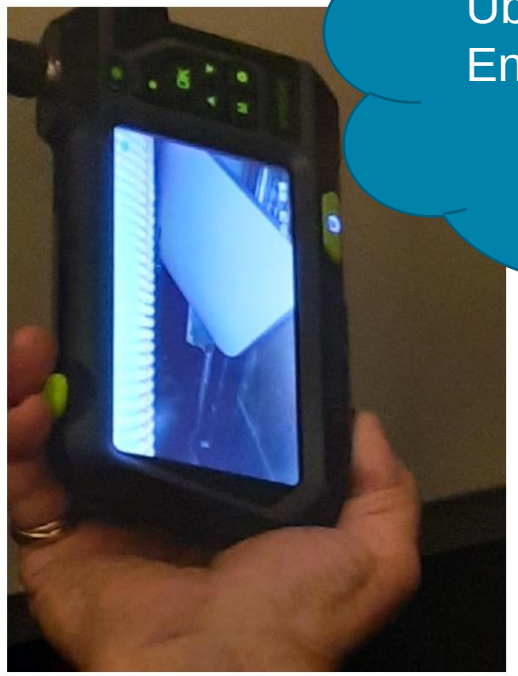
- Rückruf z.B. bei Gesprächen im Umfeld
- Frequenzen: GSM 850/900/1800/1900MHZ
- Akku-Standby-Zeit: **bis zu einer Woche**
- Akkulaufzeit bei Übertragung: bis zu 2 Stunden

Besonderes Highlight ist aber die **Geräuschaktivierung**: Registriert der Mini Audiosender im Umfeld z.B. ein Gespräch, werden Sie automatisch angerufen. Damit ergeben sich viele Einsatzmöglichkeiten im Bereich der Langzeit-Raumüberwachung.

Es gibt einen Service mit dem Namen **«Sweeping».** Hier überprüfen wir z.B. Wohnungen, Sitzungsräume, Autos auf versteckte Spionage-Tools.

Mini-Spione und GSM Mini-Sender

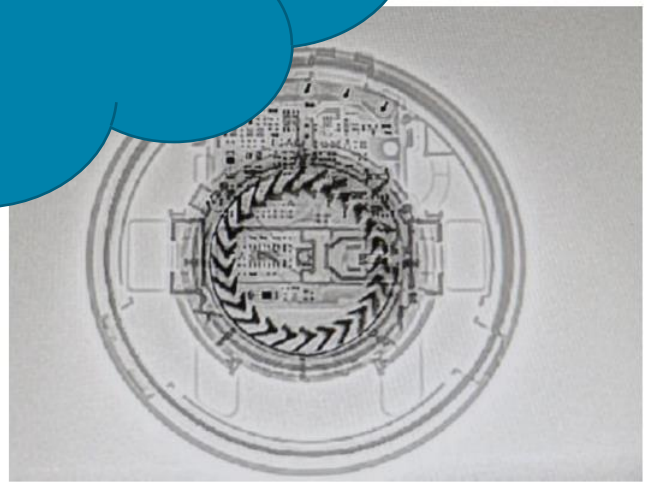


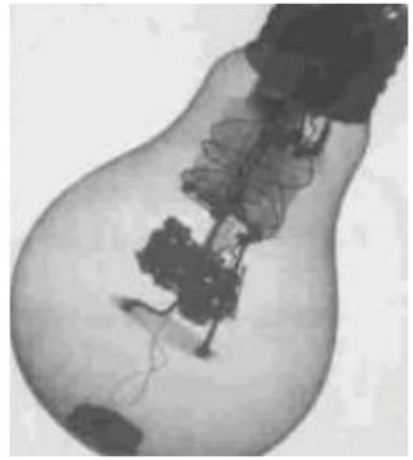


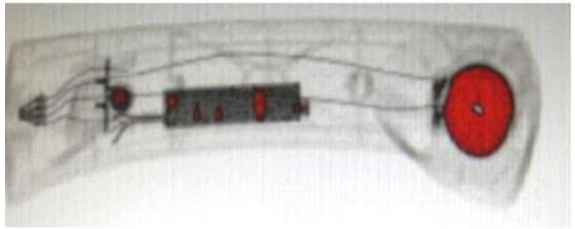
Überprüfung mit einem Endoskop.

Mini-Spione und GSM Mini-Sender

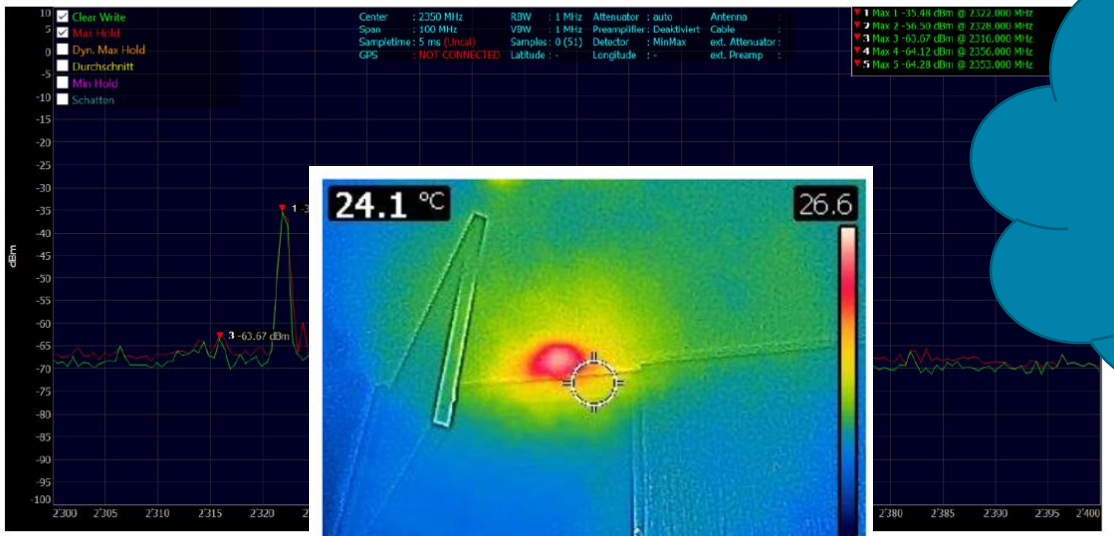
Überprüfung mit einer
mobilen Röntgen-Anlage







Mini-Spione und GSM Mini-Sender



Überprüfung mit Frequenzmessungen (SDR Empfänger mit einer speziellen Software)

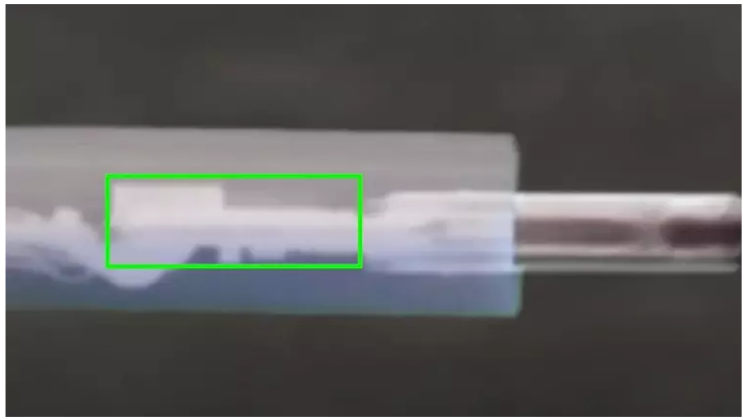
Überprüfung mit einer Thermo-Kamera

WLAN-Hotspot im Smartphone «USB Lade-Kabel»

USB-C-auf-Lightning-Kabel spioniert Nutzer aus

Eine neue Version des "OMG Cable" kann Tastenanschläge von PCs und Macs durchführen und Inhalte per WLAN-Hotspot versenden.

Lesezeit: 3 Min. In Pocket speichern 255



Miniaturisierung macht's möglich: Von Außen ist die Zusatztechnik nicht zu erkennen. (Bild: "MG")

UPDATE 06.09.2021 10:57 Uhr | Mac & i

Von Ben Schwan

Ein bekannter Hacker hat eine neue Version seines iPhone-Kabels veröffentlicht, mit dem sich Daten von verschiedenen Geräten stehlen lassen. Das sogenannte OMG Cable von Mike Grover ("MG") sieht aus wie ein reguläres, von Apple vertriebenes weißes USB-C-auf-Lightning-Kabel, wie es sie millionenfach gibt, enthält aber Elektronik, die zum Ausführen von Tastenanschlägen mit anschließendem Keylogging sowie vor allem zum Weiterversand abgefischter Inhalte verwendet werden kann. Denn ein WLAN-Hotspot ist gleich eingebaut.

[Update 08.09.21 9:50 Uhr:] Das OMG Cable mit USB-C ist im Hackerfachhandel mittlerweile erhältlich. Es kostet 140 US-Dollar. Eine Variante mit Keylogger-Funktion, die für den Anschluss an kabelgebundene Tastaturen gedacht ist, wird für 180 Dollar angeboten. Weiterhin muss ein "Programmer" erworben werden, mit dem Payloads auf das Kabel gelangen – ohne diesen ist auch ein Setup nicht möglich. Er kostet weitere 25 Dollar. Grover hat zudem ein direktionales USB-C-nach-USB-C-Kabel entwickelt, das für die Nutzung mit Android-Smartphones und Android-Tablets mit USB-C gedacht ist – sowie offenbar mit dem iPad Pro mit USB-C. (bsc)

Achten Sie darauf, wo Sie so ein USB-Kabel kaufen. Nur von einer vertrauenswürdigen Quelle. Passen Sie auf, wenn so ein USB-Kabel «geschenkt» z.B. als Werbegeschenk erhalten.

Social Engineering

Unter Social Engineering verstehen wir das Planen und Durchführen von Angriffen auf Informationen und Systeme unter Ausnutzung der «Schwachstelle Mensch».

Der Mensch ist generell hilfsbereit!

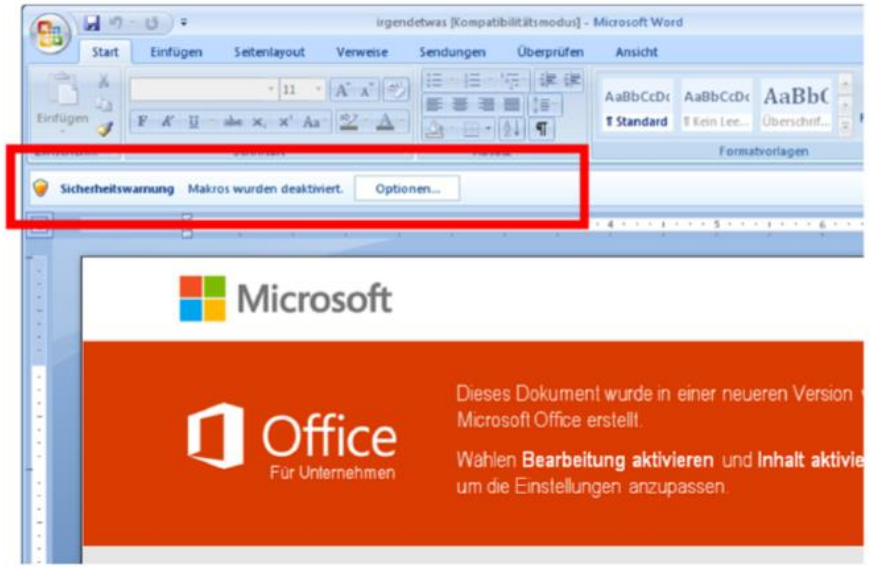
So einfach sollten Sie es dem Angreifer nicht machen!

Live getestet am 20. Juli 2013 im Kanton Luzern - Hotel «geheim» - und es funktioniert!

Doch leider wird oft schon beim Einbau geschlampt – wie wir schon in mehr als diesem einen Fall selbst feststellen mussten. Viele Hotels vergessen einfach, den vom Hersteller vorgegebenen **Mastercode (00000)** zu ändern.

Hackerangriff auf Meier Tobler AG

1. Dokument öffnet sich im geschützten Modus
2. Empfänger aktiviert Bearbeitung
3. im Hintergrund startet Makro
4. Makro lädt Emotet-Malware
5. Mai 2019



Hackerangriff auf Meier Tobler AG

Datum, Zeit	Ereignis
24.07.19 / 0200	Meier Tobler durch Provider alarmiert. Entscheid: Alle Systeme herunterfahren
24.07.19 / 0645	Krisenstab einberufen (Sofortmassnahmen, Kommunikation)
24.07.19 / 0700	Kader wird informiert, Rückholen von Schlüsselpersonen (Ferienzeit)
24.07.19 / 0800	Krisenstab bezieht «War Room», Cyber-Security Experten aufgeboten
25.07.19 / 1100	Telefonie wiederhergestellt, Not-Website online, Briefversand an MA nach Hause
26.07.19 / 1400	20 Not-Arbeitsplätze SAP in Betrieb, Kundenanfragen werden bearbeitet
27.07.19 / 1400	E-Mail-Verkehr über Webmail wiederhergestellt
28.07.19 / 1600	Betriebsaufnahme Lager Däniken und Nebikon, erste Lieferungen an Kunden

Lehren aus Cyber-Attacken

Technisch

- Zusätzliche Sicherheitsmassnahmen
- Verschärfung Policies (Anhänge E-Mail, Whitelisting Websites, Makros)
- Einführung Zwei-Faktor-Authentifizierung (2FA)
- Einführung 7x24h aktive Überwachung der Systeme (Tanium) → SOC Service
- Sandboxen zur Abklärung potenziell gefährlicher E-Mails
- Unterteilung Netzwerk in mehrere Sektoren/Domains
- Selektive Vergabe Zugriffsrechte
- Verbesserte Dokumentation Netzwerk, Systeme, Applikationen

Organisatorisch

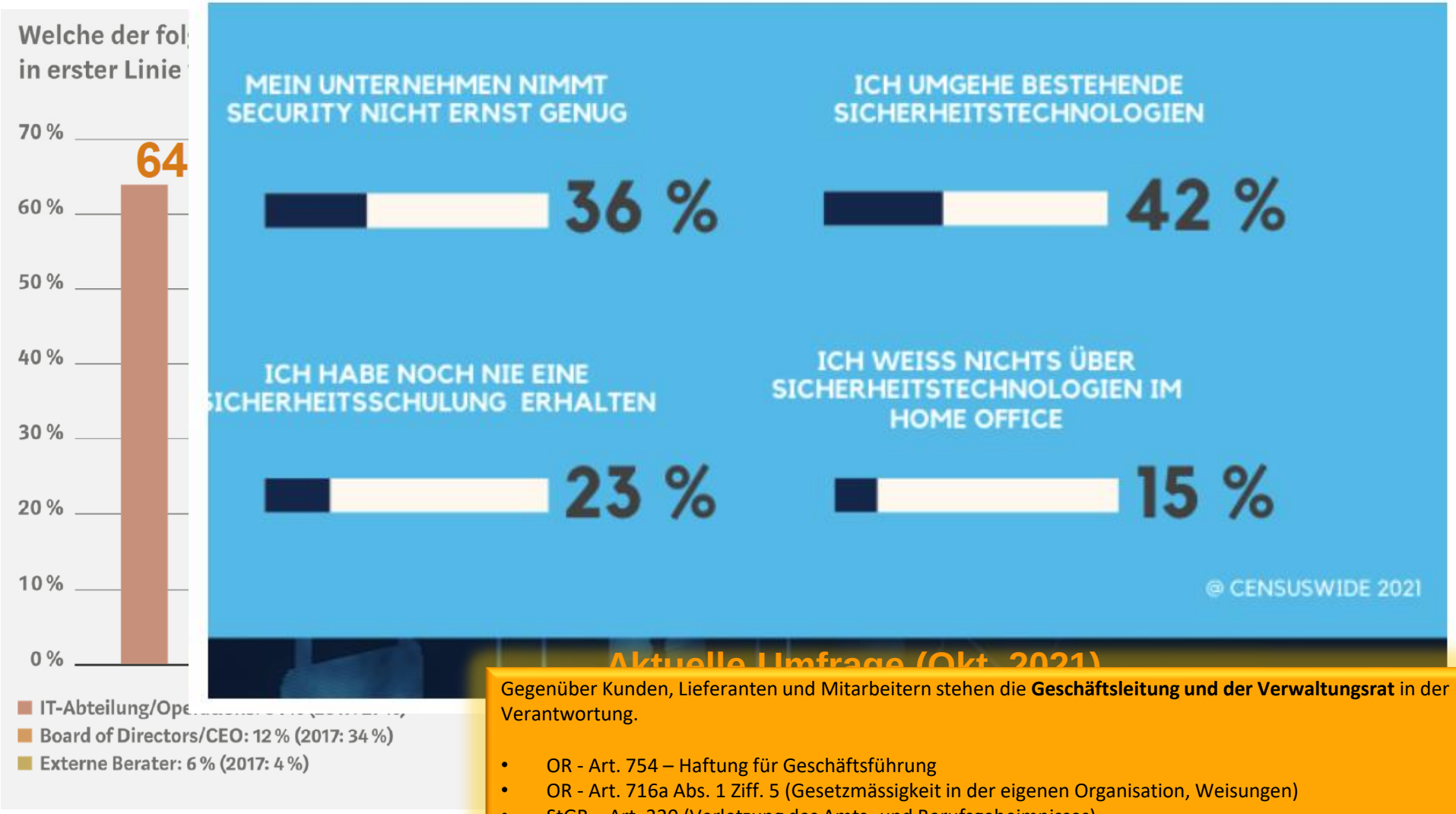
- Bedrohungslage verschärft → Sensibilisierung der Mitarbeitenden auf allen Stufen
- Notfallorganisation ≠ Krisenorganisation (Langzeit/Verfügbarkeit)
- Krisenorganisation vorbereitet und definiert
- Krisenorganisation muss periodisch optimiert und trainiert werden
- Krisenkommunikation Entscheidungswege definiert

Sichere Einführung einer Cloud-Lösung

Viele Dienstleistungen werden heute über **Cloud-Services** angeboten. Problem dabei ist, dass so ein Cloud-Service von einem Mitarbeitenden innert 5 Minuten mit einer Kreditkarte beschafft werden kann, ohne dass die IT im eigenen Unternehmen davon Kenntnis hat. Das heisst, es entsteht so eine **Schatten-IT**.

Wie löse ich als «IT Leiter» dieses Problem?

Sicherheit ist “Chefsache”



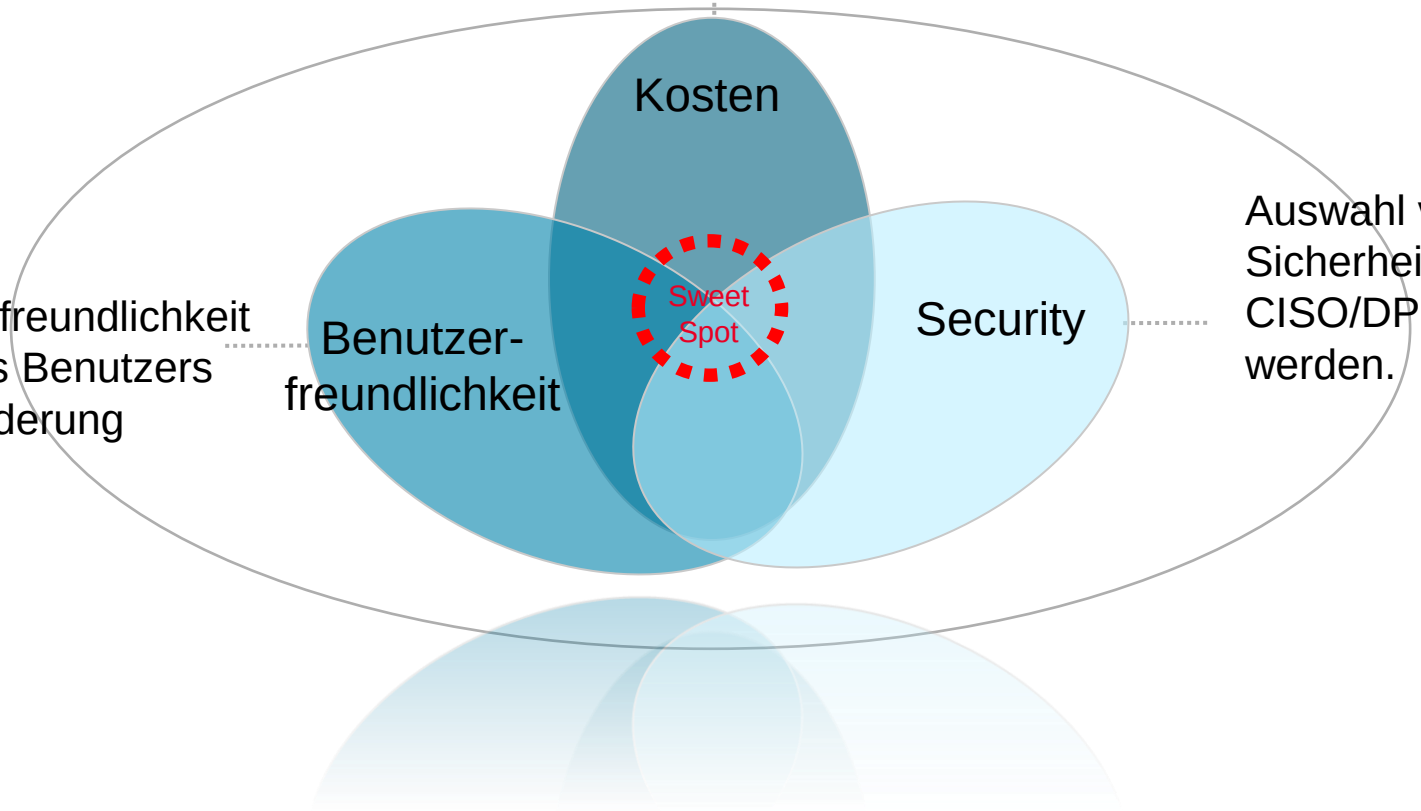
Gegenüber Kunden, Lieferanten und Mitarbeitern stehen die **Geschäftsleitung und der Verwaltungsrat** in der Verantwortung.

- OR - Art. 754 – Haftung für Geschäftsführung
- OR - Art. 716a Abs. 1 Ziff. 5 (Gesetzmässigkeit in der eigenen Organisation, Weisungen)
- StGB – Art. 320 (Verletzung des Amts- und Berufsgeheimnisses)
- StGB – Art. 162 (Verletzung des Fabrikations- oder Geschäftsgeheimnisses)
- DSG - Art. 35 (Verletzung des Datenschutzgeheimnis)

Sicherheit versus Bedienbarkeit

Abwägen des Konflikts zwischen Sicherheit, Kosten und Benutzerfreundlichkeit.

Reduzierung der gesamten Sicherheitskosten auf ein Minimum - risikobasierter Ansatz



Eine hohe Benutzerfreundlichkeit ist aus der Sicht des Benutzers die wichtigste Anforderung

Auswahl von realistischen Sicherheitsmassnahmen, die vom CISO/DPO geprüft und genehmigt werden.

Tipp:
- Fall zu Fall
- In Szenarien denken
- 80/20 Regel

Aktuelle Herausforderungen

- Cloud-Dienste, IoT Geräte, und Abhängigkeiten zu IT-Lieferanten und Schnittstellen
- Keine internen Weisungen und Sicherheitskonzepte
- Kein Notfall- und Krisenmanagementkonzept
- Hohe Komplexität – neue Gesetze (CH-DSG, DSGVO, etc.)
- Hohe Mobilität der Benutzer – Daten überall, zu jeder Zeit und auf jedem Endgerät
- Zuwenig Awareness, viel Halbwissen und Ignoranz
- Mehr und breiter motivierte und ausgerüstete Angreifer
- Mehr vernetze Werte und ein höheres Schadenpotential
- Ressourcen-Mangel und Schnelligkeit des Wandels

- Produkte lösen keine Management- und Führungsprobleme
- Bevor Sie einen Cloud-Dienst einsetzen, klären Sie wie «sicher» dieser Cloud-Provider ist.
- Haben Sie immer einen Plan «B» und hinterfragen Sie neue Projekte, Services oder Produkte in Bezug auf die Informationssicherheit und den Datenschutz

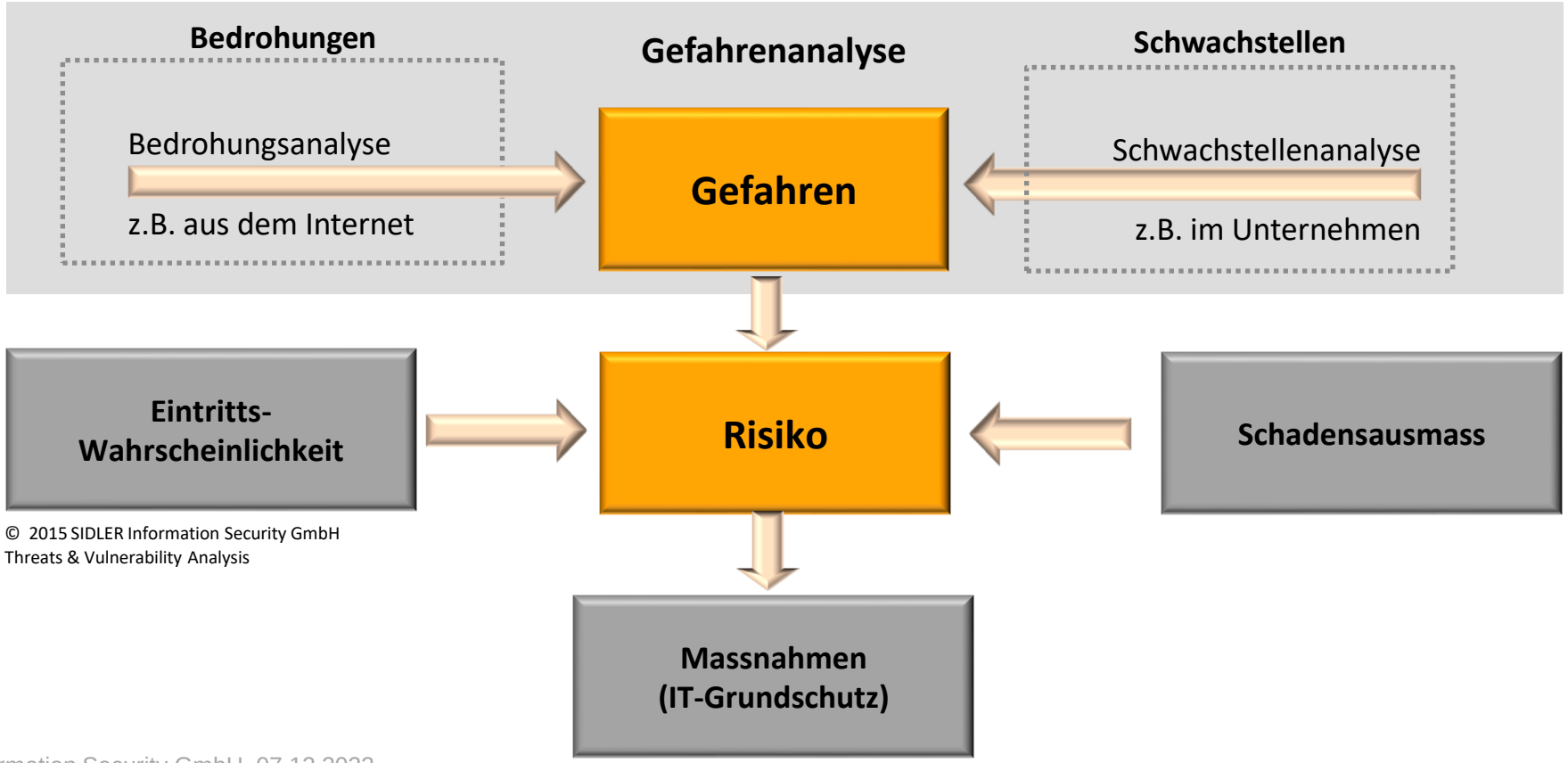
- Wie gross ist die Wahrscheinlichkeit, dass es bei Ihnen brennt? **0%**
- Wie gross ist die Wahrscheinlichkeit, dass Sie einen Cyber-Vorfall haben? **80%**

- Wer von Ihnen hat eine Feuerversicherung? **100%**
- Wer von Ihnen hat eine Cyber-Versicherung? **10%**

IT-Risiko Management

Wie entsteht ein Risiko?

- Ein Risiko ist die Gefahr, dass ein Ereignis eintrifft, das zu einem Schaden/Verlust führen kann.
- Oder ist die Gefahr, dass ein Ereignis eintrifft, das die Erreichung der Unternehmensziele beeinträchtigen oder verhindern kann.



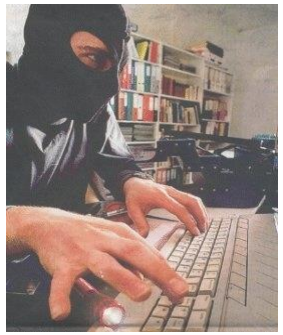
Allgemeine Gefahren und Risiken

Höhere Gewalt
Feuer, Blitz, Sturm, Überschwemmung, Stromausfall, Krankheit, …

Menschliches Versagen
Bedienungsfehler, Unwissen, falsches Verhalten, …

Gesetzliche Mängel
Nicht Einhalten der Gesetze, Reglemente etc. (Compliance)

Technisches Versagen
Netzwerkausfall, Software-Fehler, Viren, Disk-Ausfall, …



Organisatorische Mängel
Fehlende oder nicht angewendete Weisungen, unzureichende Zutrittskontrollen, falsche Zugriffsrechte, Abgang von Schlüsselpersonen (Know-how-Verlust), Versagen der Prozesse, …

Vorsätzliche Handlungen
Manipulation, Diebstahl, Missbrauch, Sabotage, Spionage, Hacking, Erpressung, Viren, organisierte Kriminalität, ...

Konsequenzen/Schaden:
- Produktions-Ausfall, Auslieferungs-Verzug, …
- Verlust von vertraulichen Daten oder Know-how
- Bussen (juristische Konsequenzen)
- Verstoss gegen vertragliche Geheimhaltungsvorschriften
- Image Schaden
- Wiederherstellungskosten

6 Schritte für eine wirksame Sicherheit

Prävention ist besser als Reaktion !

1
- Sensibilisierung aller Mitarbeitenden
- Security Newsletter
- Fingierte Phishing Attacke
- E-Learning System mit Schulungsnachweis

2
- Risiko-Management auf GL-Ebene
- jährliche Risiko-Einschätzung z.B. mit IKS
- Top 5 Risiken bearbeiten
- Massnahmen priorisieren und umsetzen
- Wirksamkeit der Massnahmen prüfen

3
- Alle Server und Clients systematisch aktualisieren
- Patch-Prozess überwachen (KPI)

4
- Alle vom Internet erreichbaren Websites wie WebShop, VPN-Portal, etc. regelmässig auf Schwachstellen prüfen lassen

5
- SOC-Anbindung und alle IP-Geräte im Netzwerk regelmässig auf Schwachstellen prüfen lassen.

6
- Mit State-of-the-Art Cyber-Security Massnahmen einen IT-Grundschutz etablieren und aufrechterhalten.

Inhalt einer IT-Nutzungsweisung mit Flyer

SIDLER Information Security

Inhaltsverzeichnis

E-Mails und Anhänge

Viren und sonstige bösartige Software werden am häufigsten verbreitet über
- E-Mails (verseuchte Anhänge)
- USB-Sticks
- Internet-Webseiten

Phishing ist eine Methode von Betrügern, um sich Informationen von ihren Opfern zu beschaffen, die zur persönlichen Bereicherung eingesetzt werden können. Phishing-Angriffe erfolgen oft via E-Mails, in denen Benutzer mit möglichst glaubhaften Geschichten dazu gebracht werden sollen, dem Absender vertraulichen Informationen auszuhändigen.

Das Wichtigste in Kürze:

- ☐ Misstrauen Sie E-Mails, deren Absender Sie nicht kennen oder deren Inhalt Ihnen verdächtig vorkommt.
- ☐ Fahren Sie mit dem Mauszeiger über die Internet-Adresse in der E-Mail, **ohne** zu klicken; so sehen Sie, auf welche Website der Link führt.
- ☐ Öffnen Sie bei verdächtigen E-Mails nie ein angehängtes Dokument oder Programm und wählen Sie keine darin angegebenen Links.
- ☐ Öffnen Sie keine Anhänge, die zwei Endungen aufweisen (z. B. foto.jpg.vbs).
- ☐ Seriöse Unternehmen fragen nie per E-Mail nach persönlichen Daten.
- ☐ Ignorieren Sie E-Mail-Aufforderungen, Ihr Passwort zu ändern.

Sorgfaltspflicht

Ihr Arbeitgeber stellt Ihnen einen gut eingerichteten Arbeitsplatz zur Verfügung, der Ihnen die tägliche Arbeit erleichtern soll. Bitte behandeln Sie die Geräte sorgfältig und mit dem nötigen Respekt.

Bearbeiten Sie Daten, so sind Sie in Ihrem Bereich für die Einhaltung von Datenschutz und Datensicherheit verantwortlich.

Fragen Sie die Security Officer, bevor Sie eine Aktion starten, bei der Sie sich über den Ausgang nicht sicher sind.

Informationen und Kontakt

Bei Fragen:
Wenden Sie sich an den Security Officer.

Für allgemeine Informatikfragen und für die Meldung von verdächtigen Vorfällen:
Wenden Sie sich an den Security Officer
max.sicherheit@firmaxy.ch, +41 41 xxx xx xx

Informationen:
Aktuelle Informationen zum Thema Datenschutz und Informatiksicherheit finden Sie in der **Richtlinie ICT-Nutzung.**

Gesetzliche Grundlage:
Schweizerisches Datenschutzgesetz (DSG)

Informationssicherheit bei Firma Muster AG

Merkblatt für den Alltag
und weiterführende Hinweise

Liebe Mitarbeiterinnen, liebe Mitarbeiter

Der Einsatz von PC, Notebook und anderen Informations- und Kommunikationsmitteln ist für uns alle eine selbstverständliche Notwendigkeit, die aber auch Risiken birgt.

Ihr Sicherheitsbewusstsein und Ihr verantwortungsvolles Verhalten ist die wichtigste Grundlage, dass diese Risiken nicht eintreten.

Dieser Flyer soll Ihnen helfen, die Risiken zu erkennen und sich richtig zu verhalten.

Ihr Security Officer
Herr Max Sicherheit
November 2019

LAB ZUG

Awareness mit «Postkarten»

SYNLAB www.synlab.ch

Clear Desk Policy

Ungeschützte Dokumente am Arbeitsplatz können in deiner Abwesenheit sehr leicht von unbefugten eingesehen oder kopiert werden. Verwahre deshalb sensible Dokumente in deiner Abwesenheit an einem sicheren versperrbaren Ort.

SYNLAB ICT-Nutzungsweisung:

- Beim längeren Verlassen des Arbeitsplatzes ist der Arbeitsplatz ordnungsgemäss aufzuräumen.
- Nicht mehr benötigte vertrauliche Dokumente sind sicher zu vernichten (Aktenvernichter). Sie gehören nicht in den Papierkorb und schon gar nicht ins Altpapier.
- Verlasse den Bildschirmarbeitsplatz nie in angemeldetem Zustand. Aktiviere die Bildschirmsperrung (Kennwortschutz). Dies gilt auch für kurze Abwesenheiten wie Toilettenbesuch, Meetings oder Raucherpausen. Bei Mehrbenutzerarbeitsplätzen (LIS-Anwendungen) sind geöffnete Programme mit besonders schützenswerten Daten zu schliessen oder zu sperren, sobald der Arbeitsplatz verlassen wird.
- Bei längerer Abwesenheit und beim Beenden des Arbeitstages ist die Citrix-Session zu schliessen und der Computer ordnungsgemäss herunterzufahren.
- Die Bürotür ist, wenn möglich, abzuschliessen.

SYNLAB www.synlab.ch

Patientenrechte

Die Labor-Ergebnisse enthalten Gesundheitsdaten, die das Datenschutzgesetz als besonders schützenswerte Daten bezeichnet. Das eidgenössische Datenschutzgesetz des Bundes gewährleistet den Schutz dieser Daten, die im Grundsatz nur mit der Einwilligung des Patienten (Kunden) bearbeitet werden dürfen. Darüber hinaus bestehen jedoch unter bestimmten Umständen (ansteckende Krankheiten, Verdacht bei Verbrechen oder Vergehen etc.) Melderechte und Meldepflichten, die uns verpflichten oder uns erlauben auch ohne Einverständnis des Patienten Daten weiterzuleiten.

Was ist zu tun?

- Die Angaben für den Labor-Auftrag wurden jeweils beim behandelnden Arzt erhoben inkl. der Einwilligung des Patienten. Wird ein Labor-Auftrag direkt in unsere Laboren entgegengenommen, müssen wir die Einwilligung bei der betroffenen Person selbst einholen. Der Patient hat dabei ein Recht auf Aufklärung über die Art und Weise der beabsichtigten Datenbearbeitung.
- Gib keine Patientendaten oder Personendaten unberechtigten Dritten Personen bekannt. Bei Unklarheiten wende dich an deinen Vorgesetzten.
- Verlangt ein Patient die Löschung oder die Einsicht seiner Befunde (Daten), muss er das entsprechende Antrags-Formular auf unserer Webseite **www.synlab.ch/datenschutz** ausfüllen.

Juni

Security Awareness - effektiv und kostengünstig !

SYNLAB www.synlab.ch

Bitte klicke keinesfalls auf **Links** oder öffne E-Mail-Anhänge, wenn du deren Herkunft nicht absolut sicher bist oder den Absender nicht persönlich kennst. Du kannst z.B. gebeten werden eine bestimmte Summe auf ein Konto zu überweisen.

Gib deine Passwörter oder Zugangsdaten **niemals** an andere Personen weiter. Niemand, auch kein Mitarbeiter der SYNLAB-IT, benötigt im Support-Fall deine Zugangsdaten.

Antworte niemals auf E-Mails, in denen du nach Passwörtern gefragt wirst, gib Passwörter keinesfalls auf Internetseiten ein, denen du nicht vertraust und reagiere skeptisch gegenüber telefonischen Nachfragen zu Zugangsdaten jeder Art.

Wende dich im Zweifelsfall immer an deinen Vorgesetzten, um Unterstützung zu erhalten.

Teste, ob du eine berechtigte E-Mail von einer Phishing-Mail unterscheiden kannst. Die Hochschule Luzern hat einen Test entwickelt mit dessen Hilfe du die Erkennung verbessern kannst.

Hier geht's zum Test:

August

SYNLAB www.synlab.ch

Social Engineering ist eine verbreitete Methode zum Ausspionieren von vertraulichen Informationen. Angriffsziel ist dabei immer der Mensch. Um an vertrauliche Informationen zu gelangen, wird sehr oft die Gutgläubigkeit und die Hilfsbereitschaft aber auch die Unsicherheit einer Person ausgenutzt. Von fingierten Telefonanrufen, über Personen die sich als jemand anderes ausgeben, bis hin zu Phishing-Attacken, ist alles möglich.

Wie sehen mögliche Social Engineering Angriffe aus?

- Eine Person gibt sich als Techniker aus (z.B. eines Labor Geräteherstellers, eine Telekomanbieters etc.) und versucht so Zugang in unser Labor zu erlangen.
- Du bekommst eine E-Mail, welche dich auffordert einen Link aufzurufen und ein Login zu tätigen oder persönliche Informationen preis zu geben **(Phishing)**.
- Eine Person ruft dich an und gibt vor eine Umfrage durchzuführen, um an sensitive Informationen (z.B. Patientendaten oder zu Sicherheitsmassnahmen etc.) zu gelangen.
- Zu deinem Arbeitsplatz kommt eine Person, die sich als Informatiker ausgibt und dir vorgaukelt, an deinem PC Wartungsarbeiten verrichten zu müssen.

Schütze dich, indem du ...

möglichst wenig persönliche Informationen über dich preisgibst. Insbesondere auf Sozialen Netzwerken wie Facebook, Xing etc. solltest du mit persönlichen Informationen sehr sparsam umgehen. Passwörter grundsätzlich nie einer anderen Person auch deinem Chef oder Systemadministrator bekanntgeben. Ein Passwort gehört dir und nur dir!

Oktober

Cyber-Versicherung

Bericht der Allianz 13.10.2021, 10:25 Uhr

Flut von Cyberangriffen macht Versicherer vorsichtiger

Die steigende Anzahl an Cyberangriffen hat auch Auswirkungen auf Versicherer, die Cyber-Policen anbieten. Sie müssen die Prämien für die Versicherungen gegen Cyberattacken anheben, wie das Beispiel der Allianz zeigt.

Versicherungsgesellschaften wie die Allianz sind in Sachen Cyber-Policen vorsichtiger geworden
(Quelle: Allianz)

Versicherer wie die Allianz halten sich bei Cyber-Policen angesichts rasant steigender Angriffe auf die Netzwerke von Unternehmen immer stärker zurück. Die Zahl der Schadenfälle bei der Allianz-Grosskunden-Tochter AGCS habe sich innerhalb von vier Jahren auf 1114 vervierzehnfacht.

Hackerangriffe in der Schweiz

Vier von zehn Firmen zahlen Lösegeld

Gemäss einer Analyse hätten Kriminelle im letzten Jahr Daten von rund 2700 hiesigen Unternehmen geklaut und zum Verkauf ins Darknet gestellt. Rund 40 Prozent der Betroffenen gingen auf die Forderungen der Hackerbanden ein.

Privileged Access Management (PAM)

E-Mail-Filterung und Web-Sicherheit

Patch-Management und Verwaltung von Sicher-

Seit dem Markteintritt 2015 habe AGCS 751 Millionen Euro für 2916 Cyber-Schadenfälle gezahlt, mehr als 80 Prozent davon nach Angriffen mit Erpresser-Software (Ransomware) oder anderen Manipulationen von aussen. Inzwischen liessen sich Cyber-Erpresser auch mieten oder nutzten den Angriff für eine ganze Serie von Erpressungen: Zur Verschlüsselung der Systeme komme dann noch die Drohung mit der Veröffentlichung erbeuteter Daten.

ZUG

Vielen Dank

«Lieber 5 umgesetzte Massnahmen als 20 geplante»