AVENIQ

Information Security in Healthcare

Aktuelle Bedrohungslage und wie Sie Ihre Mitarbeitenden sensibilisieren

Clemens Chizzali-Bonfadin
Patrick Gürtler

21. September 2021

Inhalt

Information Security in Healthcare

- → Wer wir sind
- → Ausgangslage
- → Cyber Threat Landscape
- → Awareness ganz gezielt
- → Zusammenfassung

Wer wir sind

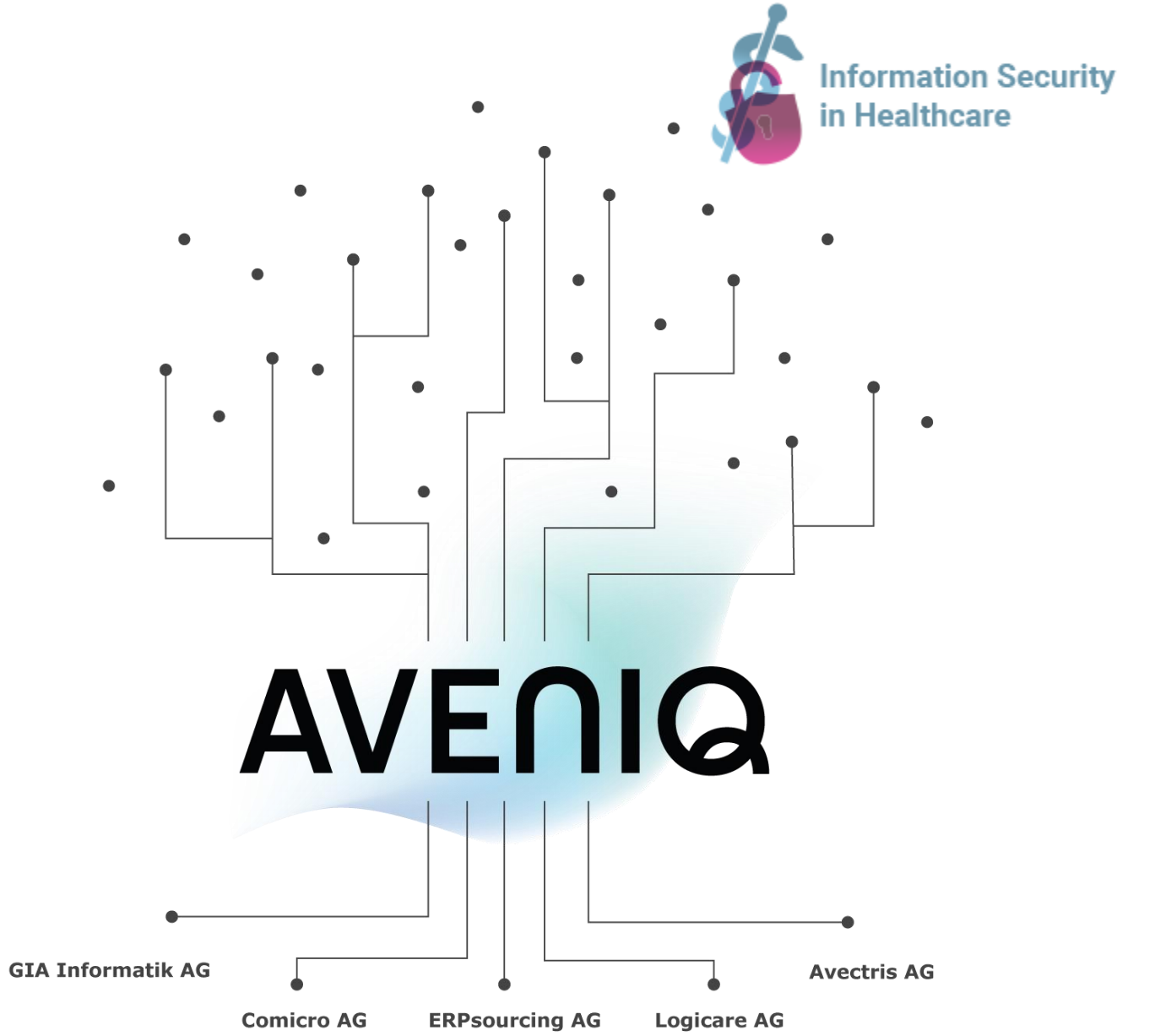
Vorstellung

Information Security in Healthcare

Clemens Chizzali-Bonfadin
Expert Consultant

Patrick Gürtler
Senior Consultant

Woher wir kommen



Über Aveniq

Aveniq gehört zu den grössten Schweizer IT-Dienstleistern und bündelt die langjährige Erfahrung und das Know-how der über 600 Mitarbeitenden.

- → breites Dienstleistungsangebot
- → Vielzahl von Experten
- → Know-how aus zahlreichen Kundenprojekten
- → Best-Practices aus verschiedenen Branchen
- → enge Zusammenarbeit mit strategischen Partnern und Herstellern
- → alles aus einer Hand
- → Partner auf Augenhöhe

Gemeinsame Power

Information Security in Healthcare

Standorte	Baden, Dübendorf, Oftringen
Mitarbeitende	> 630 Experten
Kunden	über 400 Unternehmen die uns das Vertrauen schenken
Projekte	über 490 Erfolgsgeschichten jährlich
Zertifikate Aveniq	ISO 20000-1:2018 «IT Service Management» ISO 27001:2013 «Informationssicherheit»
Zertifikate Aveniq Avectris	ISO 22301:2012 «Aufrechterhaltung der Betriebsfähigkeit» ISO 27001:2013 «Informationssicherheit»
Umsatz	180 MCHF

Portfolio

Information Security in Healthcare

Architecture	Cloud	Security		
AI	Chatbot	DevOps	RPA	
BPS	CMS	Collaboration	Health	
Legal	PLM	SAP S/4HANA	Utilities	
Basic Services	Cloud & Datacenter	Hybrid	Modern Workplace	
OnPrem	Privat Cloud	Public Cloud	SAP	Security & Connectivity

Beraten
Wir beraten Sie in Bezug auf IT-Einsatz, Technologie und Sicherheit.

Automatisieren
Wir automatisieren Prozessschritte und Kundeninteraktionen.

Digitalisieren
Wir digitalisieren Zusammenarbeit und Business-Prozesse.

Betreiben
Wir unterstützen Sie in IT-Systemintegration und IT-Betrieb.

Referenzen

Information Security in Healthcare

Dienstleister	Finanzwirtschaft	Gesundheitswesen	Recht	Industrie	Öffentlicher Sektor	Versorger
DENNER	Basler Kantonalbank	Claraspital – In besten Händen.	Homburger	Angst+Pfister	STADT BADEN	axpo
SUISA	GENERALI	KSB	BÄR & KARRER	AGATHON SWITZERLAND	University of Zurich[UZH]	STADTWERK WINTERTHUR
Hotelplan	Schroders	SWICA	walderwyss rechtsanwälte	SWISSPHONE	nw Fachhochschule Nordwestschweiz	EKZ
Livit	EY	Balgrist Universitätsklinik	PESTALOZZI ATTORNEYS AT LAW	RONDO Dough-how & more.	Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra – Eidgenössisches Departement für auswärtige Angelegenheiten EDA	SIG
swissport	Zürcher Kantonalbank	Überall für alle SPITEX Zürich Limmat	NKF	HUBER+SUHNER Excellence in Connectivity Solutions	Stadt Winterthur	swissgrid

Ausgangslage

Einführung

Information Security in Healthcare

Cyber-Sicherheit ist bereits unter üblichen Umständen eine Herausforderung.

In der turbulenten Zeit, der weltweiten Pandemie, die zu dramatischen Veränderungen in beruflichen Umgebungen führt, kann sie unmöglich erscheinen.

IT-Sicherheitsexperten erlebten unter anderem folgendes:

→ eine Lawine von Phishing-Betrug mit Corona-Virus-Bezug

→ eine Flut von Ransomware-Angriffen

→ Sicherstellen der Sicherheit der Anwender*innen nach dem abrupten Wechsel ins Homeoffice

Es passiert tatsächlich

Information Security in Healthcare

Kontakt | E-Paper | Abo | Shop | Mediadaten

IT-MARKT

NEWS STORYS DOSSIERS VIDEO SPECIALS

NEWS

Was IT-Security-Experten den Schlaf raubt

Falsche Bluemail-App ködert Swisscom-Kunden

Fr 25.10.2019 - 12:21 Uhr
von Coen Kaat

Komisch, spannend und beängstigend. Jeden Tag kommen neue Meldungen zu DDoS-Attacken, Ransomware, Cryptominern und Co. Die Redaktion bloggt an dieser Stelle über alles rund um Cybercrime und IT-Security.

(Source: Coen Kaat)

TICKER

25.10.2019 - 12:21 Uhr

Falsche Bluemail-App ködert Swisscom-Kunden

SHARE

swiss cloud computing ag: Update zur Bereinigu der Cyberattacke

30.4.21,16:30h + Die swiss cloud computing AG, ein Schweizer Cloud-Provider für unabhängige Software-Anbieter (ISV) und ICT-Reseller wurde, wie mitgeteilt, am 27. April Opfer einer gezielt Cyberattacke. Das Unternehmen ist zuversichtlich, dass die Systeme im Verlauf der kommende wieder für die Kunden verfügbar sein werden.

https://www.inside-it.ch/de/post/ransomware-angreifer-forderten-mehrere-millionen-von-griesser-20210427

< Zurück zur Startseite

Ransomware-Angreifer forderten mehrere Millionen von Griesser

SECURITY, INDUSTRIE, ATTACKE, CYBERCRIME, GRIESSER, SCHWEIZ,

Von Katharina Jochum, 27. April 2021 17:41 Letzte Aktualisierung: 28. April 2021 14:55

Foto: Griesser

Der Schweizer Industriefirma wurden Daten entwendet. Sie will sich den Kriminellen aber nicht beugen.

Cyber-Kriminelle lieben Krisen

Information Security in Healthcare

From [redacted]

Reply | Reply All | Forward | More

Subject **Remedies On Corona-Virus**

23/02/2020 à 15:00

Reply to [redacted]

Dear Reader,

A group of Corona-Virus Specialist is here in our own direct contact clinical attachedl for an antiviral called remdesivir.

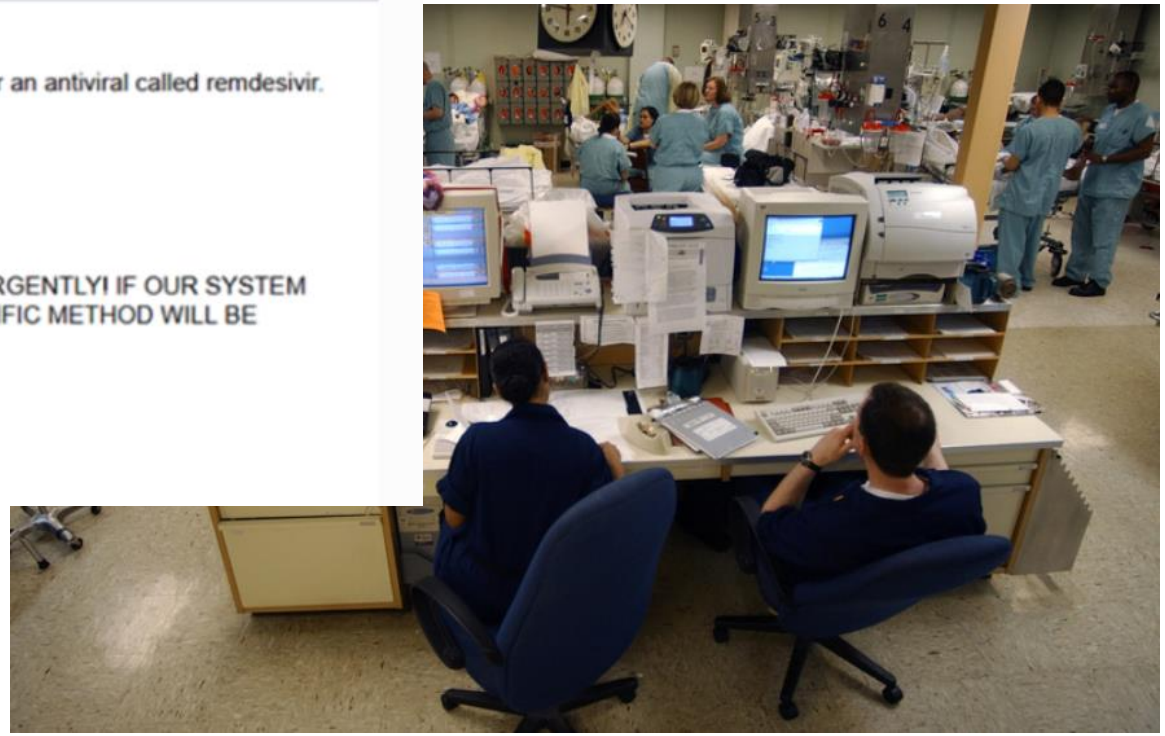
Attached is step one 10$ to connect with on Skype

Skype: live:.cid.e63ddc29b41078e7

Note: If you have an active email then your reply is needed. PLEASE PAY THE BTC URGENTLY! IF OUR SYSTEM DOES NOT RECEIVE YOUR PAYMENT WITHIN 7 DAYS. ALL DATA FOR THE SPECIFIC METHOD WILL BE TERMINATED PERMANENTLY FOR YOUR DOWNLOAD.

1Kw5qE92mSehKJ9AHjXRh44q2u2wgxZ86Z

log in to your account | get support



Heutige Herausforderungen

Information Security in Healthcare

Die Aufgaben im Bereich Informationssicherheit werden ständig komplexer und aufwendiger.

- Hochentwickelte und häufigere Cyber-Angriffe
- Ständig wechselnde Cyber-Bedrohungslandschaft
- Digitalisierung bringt neue Sicherheits-herausforderungen mit sich
- Immer komplexere IT-Landschaften zu managen
- Gesetzliche Anforderungen

Die Cyber-Sicherheit wirkt sich auf die Unternehmen auf vielfältige Weise aus.

- Management (Verantwortlichkeiten, Strategische Entscheide, Ressourcen etc.)
- Prozesse (Incident Management, Business Continuity, Risk Management, Vulnerability Management etc.)
- Leute (Sicherheitsbewusstsein, Schulungen, Kommunikation etc.)
- Systeme (IT-Hygiene, Konfiguration, Asset Management)
- Daten (Vertraulichkeit, Backup etc.)

Eine holistische Methodik ist notwendig, um immer komplexere Cyber-Sicherheitsszenarien erfolgreich zu managen

Cyber-Security ist kein Technikprodukt

Information Security in Healthcare

→ Technologie alleine kann das Problem nicht lösen

→ Das menschliche Verhalten und funktionierende Sicherheits-Prozesse sind wichtige Faktoren

Der Weg des geringsten Widerstands

Information Security in Healthcare

Cyber Threat Landscape

Cyber Threat Landscape Report

→ Der Bericht fasst die **wichtigsten Ereignisse des letzten Monates** im Bereich Cyber Security zusammen und enthält **nützliche Empfehlungen**.

→ **Anwendungsfälle**

- Übersicht der aktuellen Cyber-Bedrohungen und –Tendenzen
- Wiederverwendung des Inhalts zur Darstellung der Cyber-Risikolage vor dem Senior Management / Verwaltungsrat
- Wiederverwendung des Inhalts zur Sensibilisierung Ihrer Mitarbeitenden
- Informationen zur Umsetzung, um das Risiko durch aktuelle Cyber-Bedrohungen zu reduzieren

→ **Zielpublikum**: CIO, CISO, IT-Sicherheitsbeauftragte, IT-Leiter, Security Teams

Inhalt des Cyber Threat Landscape Report

Information Security in Healthcare

Beispiel eines Cyber Threat Landscape Reports 1/3

Information Security in Healthcare

Zusammenfassung des Monats 1/2

Zusammenfassung

Der Angriff über Kaseyas Software-Management stellt eine neue Qualität der Ransomware-Angriffe dar. Denn damit erreichte die REvil-Gang nicht nur über 1000 Firmen auf einen Schlag, sie traf auch Firmen, die eigentlich gar keinen Fehler gemacht hatten. A
andere Sicherheitslücken hatten dies
konnten. Stattdessen erfolgte der An
Supply-Chain- oder Lieferkettenangr

Comparis ist Opfer einer Ransomwar
beziehungsweise bewusst heruntergе
Cyberkriminellen ein «Lösegeld» für
forderten die Täter 400'000 Dollar. C
Zeit konnten die Systeme abgesicher
Einige Tage später gab es ein Update
sind auch Kundendaten entwendet w
erbeuteten Daten seitens der Angreif
Kontaktaufnahmen kommen, bei der

Hacker verschicken eine personalisie
Michael Page hätte ein attraktives Jo
Mit einem persönlichen E-Mail, das d
ein sehr nettes Feedback über den E
offene Stelle sprechen. Aus Daten- u
senden. Das E-Mail enthält dann auc

Beobachtete Trends im Juni 2021 (Weltweit)

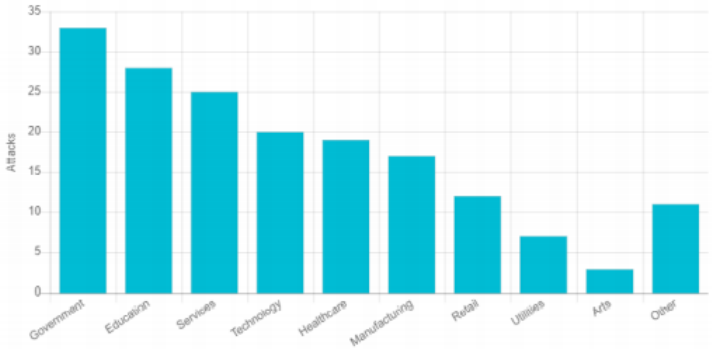
Bedrohungstypen	Vergleich zu Mai 2021	Vergleich zu Juni 2020
Malware	↓	→
Intrusionen	→	↑
Ransomware	↑	↑
Phishing	→	↓
Web App Angriffe	↑	↑
Cryptojacking	→	↑
IoT Malware	↓	↑

↓ Abnehmend
→ Stabil

kritisch
hoch
mittel
tief

Index der Gesamtbedrohung (- 2% im Vergleich zum letzten Monat)

Ransomware nach Industrien



Beispiel eines Cyber Threat Landscape Reports 2/3

Information Security in Healthcare

Thema des Monats 1/3

Kaseya VSA: Wie die Lieferketten-Angriffe abliefen – 04.07.2021

https://www.heise.de/hintergrund/Kaseya-VSA-Wie-die-Lieferketten-Angriffe-abliefen-und-was-sie-fuer-uns-bedeuten-6129656.html

Der Angriff über Kaseyas Software-Management stellt eine neue Qualität der Ransomware-Angriffe dar. Denn damit erreichte die REvil-Gang nicht nur über 1000 Firmen auf einen Schlag, sie traf auch Firmen, die eigentlich gar ke verwundbare VPN-Dienste oder andere Sicherheitslücken hatten diese Op Stattdessen erfolgte der Angriff über ganz reguläre Prozesse, wie sie jede heimtückisch.

Kaseya VSA ist eine Plattform für das Management von Software. Zu der dieser Management-Software gab es offenbar mehrere Lücken, die zumin gemeldet wurden. Doch der aktuelle Angriff am 2. Juli erfolgte, noch bev Angriff, obwohl der Hersteller zumindest einen Teil der Lücken bereits ka man aus dem Internet ohne Authentifizierung mit der Server-Software « Zugriffe auf */dl.asp/KUpload.dll/userFilterTableRpt.asp* mit dem Komman eine SQL Injection auslösen, also Datenbank-Befehle einschleusen. Die fü ausführen konnten. Damit kontrollierte die REvil-Bande Server, deren Au nutzte sie weidlich aus.

Die Angreifer kopierten eine alte Version des Windows Defender (Version Start lädt sie die Bibliothek *mpsvc.dll* aus dem aktuellen Verzeichnis. Dur gleichnamige Systembibliothek aus *system32/*, sondern um den eigentlic System. Durch den Umweg über das verwundbare Defender-Binary gesch Microsoft-Signatur.

Cyber Angriffe des Monats 2/2

Kaseya: Rund 1.500 Unternehmen von REvil-Ransomware-Angriff betroffen – 04.07.2021

https://www.bleepingcomputer.com/news/security/kaseya-roughly-1-500-businesses-hit-by-revil-ransomware-attack/

Kaseya sagt, dass der REvil-Ransomware-Angriff die Systeme von etwa 60 seiner direkten Kunden, die das VSA-Produkt des Unternehmens vor Ort nutzen, angegriffen hat. Insgesamt weiss der Anbieter von Cloud-basierter MSP-Software von bis zu 1.500 Opfern, deren Netzwerke von MSPs mit Kaseya Remote-Management-Tools verwaltet wurden. Das Unternehmen stellt Netzwerk- und Endpunkt-Indikatoren für Kompromittierungen (IOCs) zur Verfügung, um Sicherheitsforschern und Kunden bei ihren Untersuchungen zu helfen, sowie eine aktualisierte Version seines Compromise Detection Tools, um Systeme auf Anzeichen von Sicherheitsverletzungen zu überprüfen.

Um Ransomware-Payloads auf den Systemen von Kaseya-Kunden und deren Kunden zu installieren, nutzten die REvil-Betreiber eine Zero-Day-Schwachstelle (CVE-2021-30116) in Kaseya VSA, einer RMM-Software (Remote Monitoring and Management), die häufig von MSPs zur Verwaltung von Kundennetzwerken verwendet wird. REvil behauptet nun, mehr als 1.000.000 Systeme verschlüsselt zu haben und verlangt nach einer ersten Forderung von 70 Millionen Dollar nun 50 Millionen Dollar für einen universellen Entschlüssler.

Coop-Supermarkt schliesst 500 Filialen nach Kaseya-Ransomware-Angriff – 03.07.2021

https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/

Die schwedische Supermarktkette Coop hat ca. 500 Filialen geschlossen, nachdem sie von einem REvil-Ransomware-Angriff betroffen war, der über eine Supply-Chain-Attacke auf Managed Service Provider abzielte. Kurz nach dem Angriff veröffentlichte Coop eine Mitteilung, dass alle Filialen mit Ausnahme derjenigen in fünf Regionen geschlossen wurden, nachdem die Kassen aufgrund eines «IT-Angriffs» auf einen ihrer Lieferanten nicht mehr funktionierten.

Es ist nun bekannt, dass sie von dem Kaseya-Cyberangriff betroffen waren, der es der Ransomware REvil ermöglichte, die Systeme ihrer Kunden zu verschlüsseln. Kaseya gab an, dass REvil eine Schwachstelle in ihrem VSA-Service vor Ort nutzte, um den Angriff auszuführen, und dass in Kürze ein Patch veröffentlicht werden würde.

Beispiel eines Cyber Threat Landscape Reports 3/3

Information Security in Healthcare

Schwachstellen des Monats 2/3

Microsoft gibt Hinweise zu einer neuen Sicherheitslücke im Windows Print Spooler – 18.07.2021

https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-guidance-on-new-windows-print-spooler-vulnerability/

Microsoft gibt Hinweise zur Behebung einer neuen Windows Print Spooler-S
gegeben wurde und bei der es sich um eine Anfälligkeit für die Erhöhung vo
kürzlich gepatchten Sicherheitslücke PrintNightmare kann diese Sicherheits
erlangen.

Microsoft hat zwar keine Sicherheitsupdates veröffentlicht, um diese Schwa
denen Administratoren Angreifer daran hindern können, die Schwachstelle
Dienst auf einem anfälligen Gerät zu deaktivieren.

SolarWinds-Hacker nutzten iOS 0-Day aus, um iPhones zu kompron

https://www.hackread.com/solarwinds-hackers-ios-zero-day-hack-iphones/

Die jüngste Enthüllung ist, dass die Hacker von SolarWinds von einer iOS-Z
erfahren und diese ausgenutzt haben, um aktualisierte iPhones zu kompron
Dieser Cyberangriff war Berichten zufolge Teil einer E-Mail-Kampagne, die
Regierungen zu stehlen. Die Hacker schickten Nachrichten an Regierungsve
13.7 abgesehen. In dieser Kampagne leiteten sie die Nutzer auf Domains u

Diese Payloads hatten die Aufgabe, Authentifizierungs-Cookies von verschie
Die Daten wurden später über einen WebSocket an den Hacker gesendet.

Tactics, Techniques & Procedures 3/3

Neue BIOPASS-Malware streamt live den Bildschirm des Opfers – 13.07.2021

https://www.bleepingcomputer.com/news/security/new-biopass-malware-live-streams-victims-computer-screen/

Hacker haben Glücksspielseiten kompromittiert, um einen neuen Remote-Access-Trojaner (RAT) namens BIOPASS einzuschleusen, der es ermöglicht, den Computerbildschirm des Opfers in Echtzeit zu beobachten, indem er beliebte Live-Streaming-Software missbraucht. Abgesehen von dieser ungewöhnlichen Funktion, die zu den üblichen Funktionen von RAT hinzukommt, kann die Malware auch private Daten aus Webbrowsern und Instant-Messaging-Anwendungen stehlen.

Trojaner kommt als angebliches Jobangebot im Namen von Michael Page – 06.07.2021

https://www.cybercrimepolice.ch/de/fall/trojaner-kommt-als-angebliches-jobangebot-im-namen-von-michael-page/

Hacker verschicken eine personalisierte E-Mail an Nutzer, in der sie vorgeben, die renommierte Stellenvermittlung Michael Page hätte ein attraktives Jobangebot: «Was sind Ihre Interessen oder Hobby ausserhalb der Arbeit?». Mit einem persönlichen E-Mail, das den Namen des Empfängers enthält, wird das Opfer angesprochen. Man hätte ein sehr nettes Feedback über den Empfänger erhalten und wolle in einem persönlichen Gespräch über eine offene Stelle sprechen. Aus Daten- und Persönlichkeitsschutzgründen könne man das Angebot nur verschlüsselt senden. Das E-Mail enthält dann auch einen Link auf eine Datei, die der Empfänger herunterladen soll: JOB BESCHREIBUNG für «Name des Opfers». Klickt das Opfer auf die beiden gelben Balken im entpackten Excel, so wird nicht wie suggeriert die geschützte Ansicht freigegeben, sondern der Trojaner Ursnif (aka Gozi, Dreambot) installiert sich auf dem Computer des Opfers. Ab jetzt können die Hacker das E-Banking des Opfers mitverfolgen und haben Zugriff auf die Tastatureingaben, den Bildschirm und die Kamera des PC.

Babuk Ransomware-Bande ist wieder in Aktion – 04.07.2021

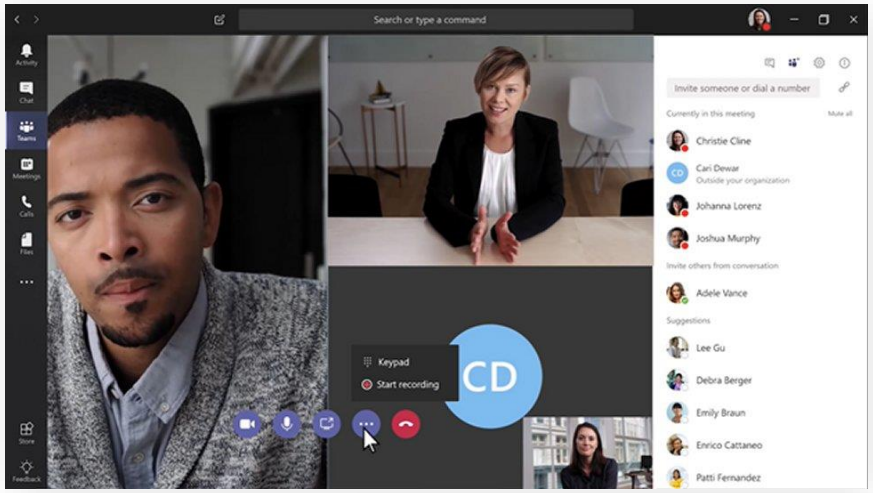
https://www.itsecuritynews.info/babuk-ransomware-gang-is-back-into-action

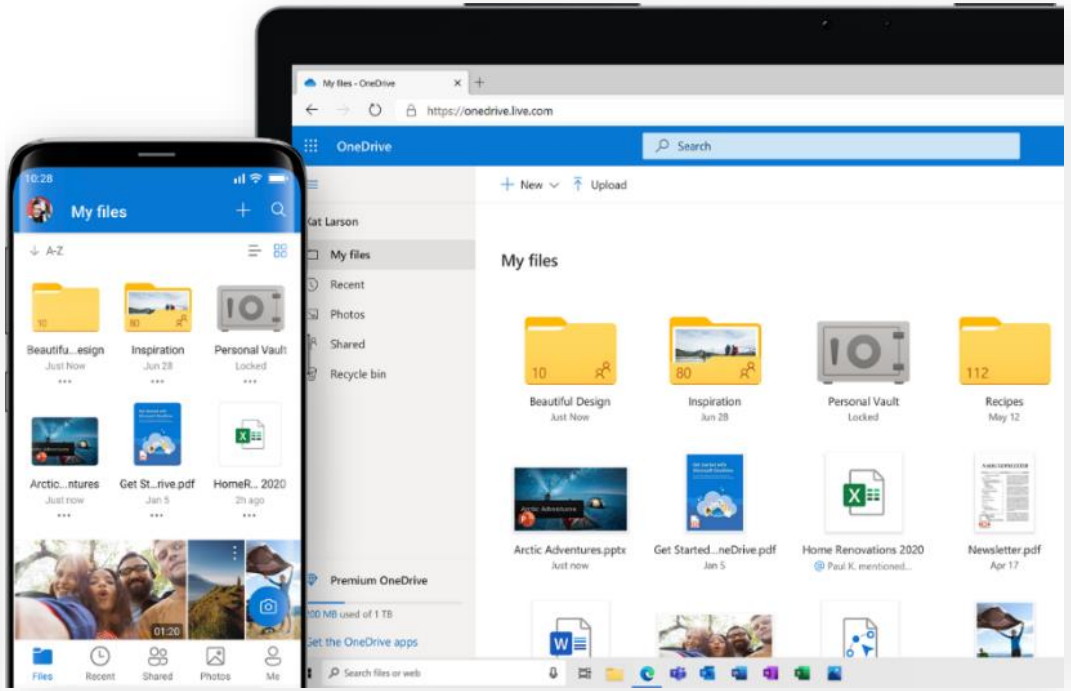
Obwohl sie ihren Rückzug aus dem Unternehmen erklären, scheinen die Betreiber der Babuk-Ransomware mit einem neuen Angriff auf Unternehmensnetzwerke in alte Gewohnheiten zurückgefallen zu sein. Die Hacker verwenden derzeit eine neue Version ihrer dateiverschlüsselnden Malware und haben ihre Aktivitäten auf eine neue Leak-Website verlagert, auf der eine Handvoll Opfer identifiziert wird. Die Gruppe erklärte ausserdem, dass sie ihre Malware weitergeben wolle, um anderen Cyberkriminellen den Einstieg in einen Ransomware-as-a-Service-Betrieb zu ermöglichen. Die Bedrohungsakteure hielten ihr Versprechen und veröffentlichten ihren «Builder», ein Tool zur Erstellung massgeschneiderter Ransomware.

Awareness ganz gezielt

2020: Der Mensch wurde zum Perimeter

Information Security in Healthcare

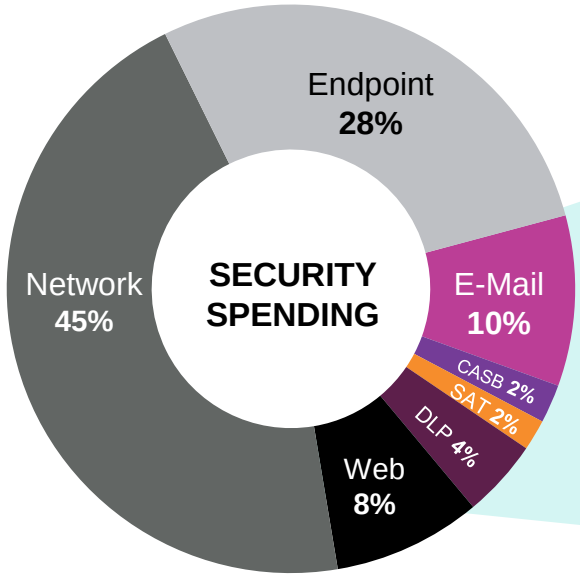




Angreifer fokussieren auf den Menschen …

Information Security in Healthcare

… die meisten Abwehrmechanismen zielen aber nicht darauf.



Source: Gartner Information Security, Worldwide 2019–2025, 4Q 2020 update (2021 forecast)

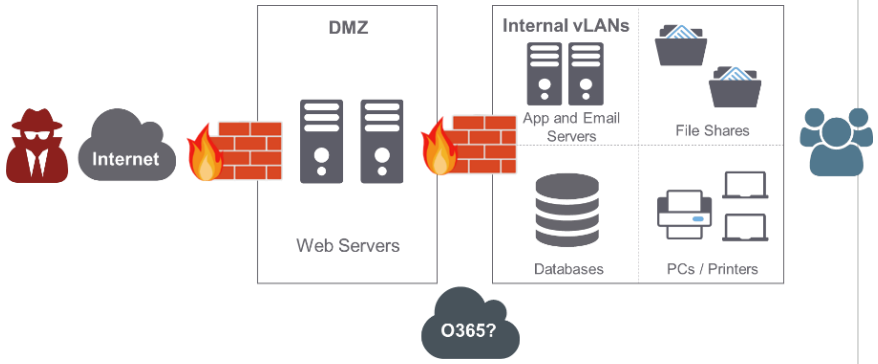
Source: 2020 Verizon DBIR

Verteidigung den Angreifern anpassen

Information Security in Healthcare

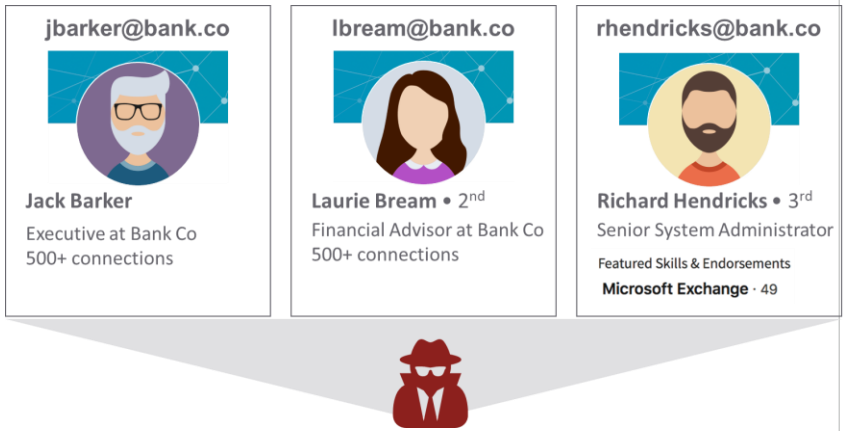
Klassischer Ansatz

Schutz von Geräten, Netzen etc.



Angriffs-Strategie

Menschen ins Ziel nehmen



Menschenzentriertes Ökosystem

Information Security in Healthcare

Vulnerability

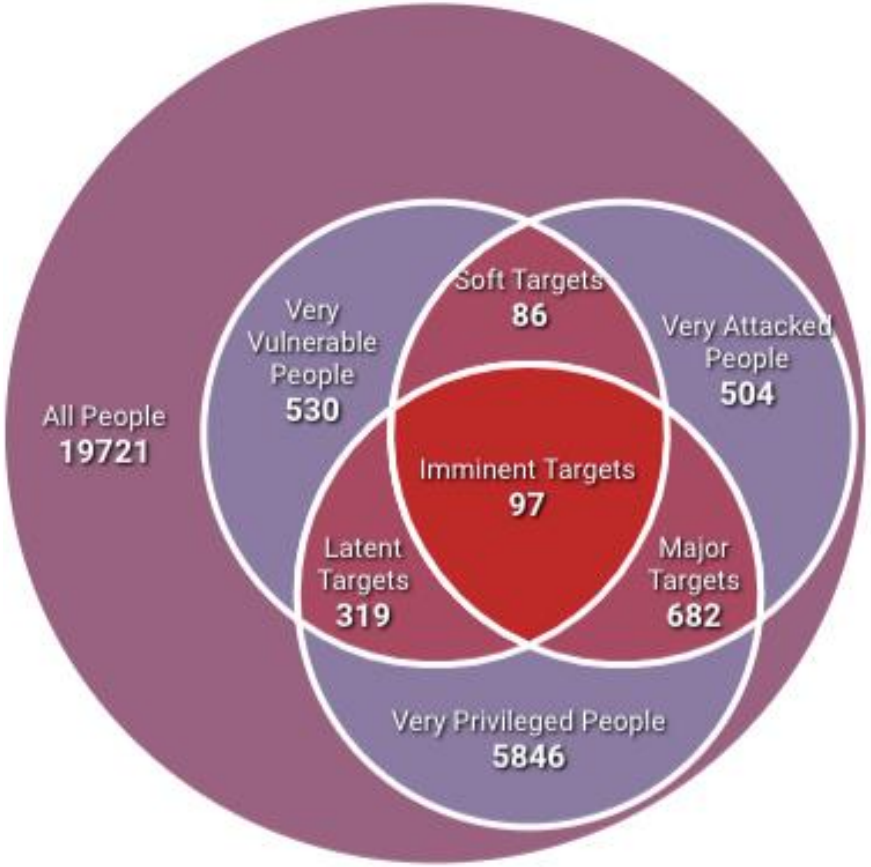
Wer fällt am ehesten auf Angriffe herein?
Klickt auf bösartige Inhalte, versäumt Awareness-Schulungen oder nutzt riskante Geräte oder Cloud-Dienste

Attack

Wer wird ins Visier genommen?
Wird sehr gezielt, ausgeklügelt oder häufig angegriffen

Privileges

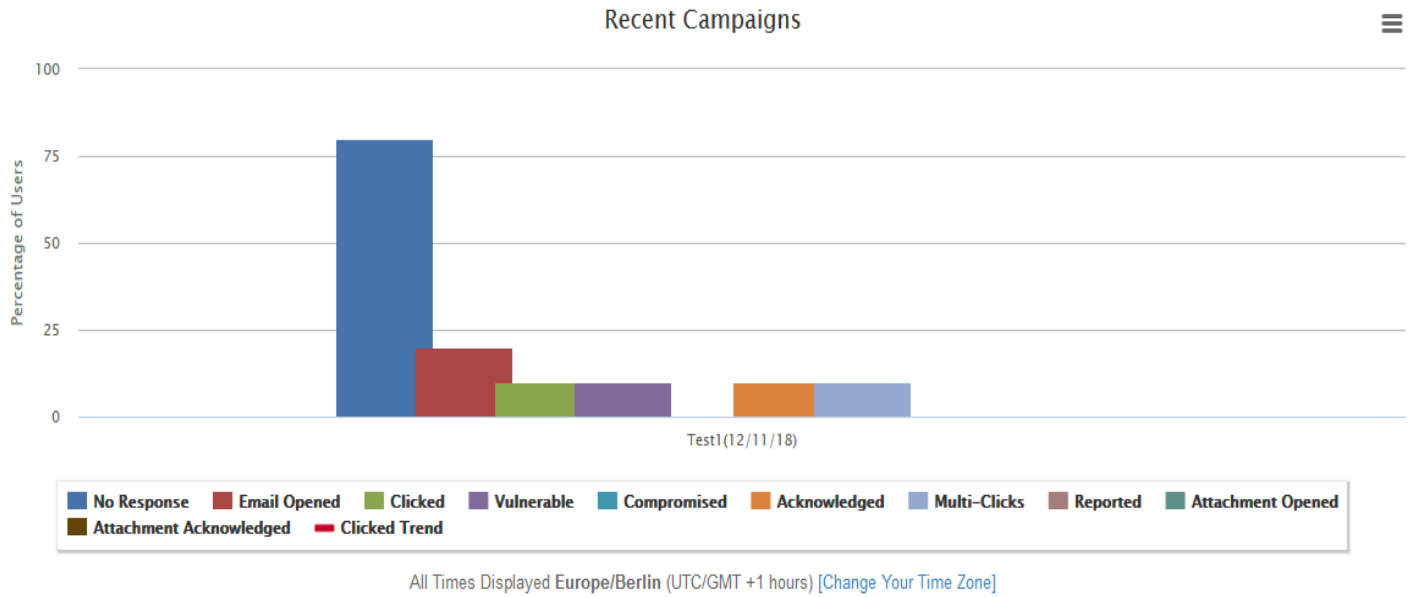
Wer stellt ein hohes Risiko dar?
Kann auf kritische Systeme oder sensible Daten zugreifen oder kann ein Vektor für laterale Bewegungen sein



Auswertungsmöglichkeiten Assessments

Information Security in Healthcare

Anhand der Ergebnisse aus dem Assessment können massgeschneiderte Schulungen an die Mitarbeitenden versendet werden.



All Email Campaign History 1

All | Pending | Running | Completed | Show As | Export Data

	Title	Sent	Opened	Clicked	Vulnerable	Compromised	Multiclick	Acknowledged	Attachment Opened	Attachment Acknowledged	Reported	Created	Start	End	Status	Creator
	Test1 From: Voicemail System	10	2	1	1		1	1	0	0	0	12/11/18 2:16:36 PM	12/11/18 2:16:36 PM	12/19/18 11:00:00 PM	Running	Tamdin Lhasam

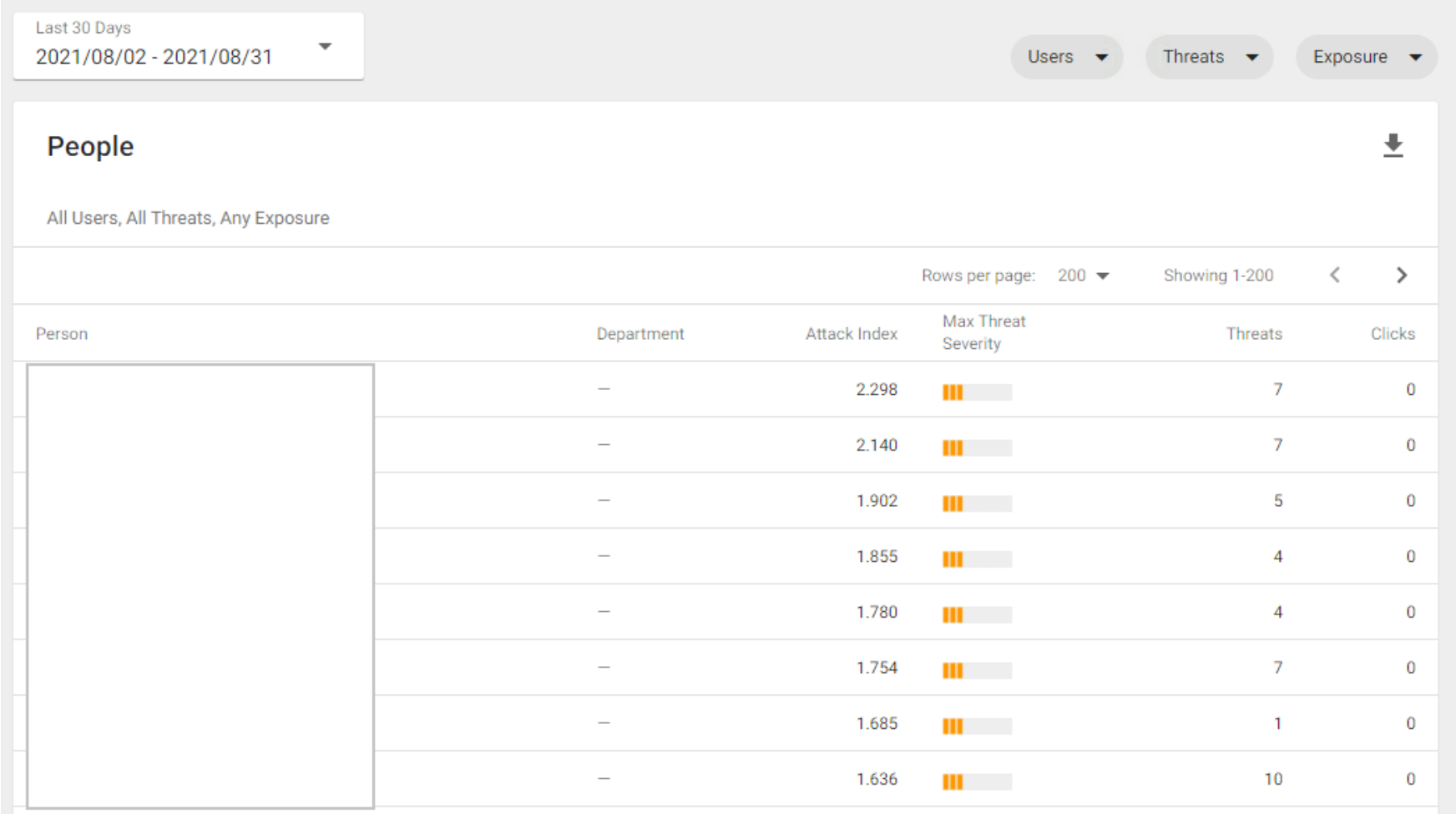
VAP – Very Attacked People (Mail-Security)

Information Security in Healthcare

Attack Index basiert auf
3 Key-Komponenten:

- Angreifer
- Ziel
- Bedrohung

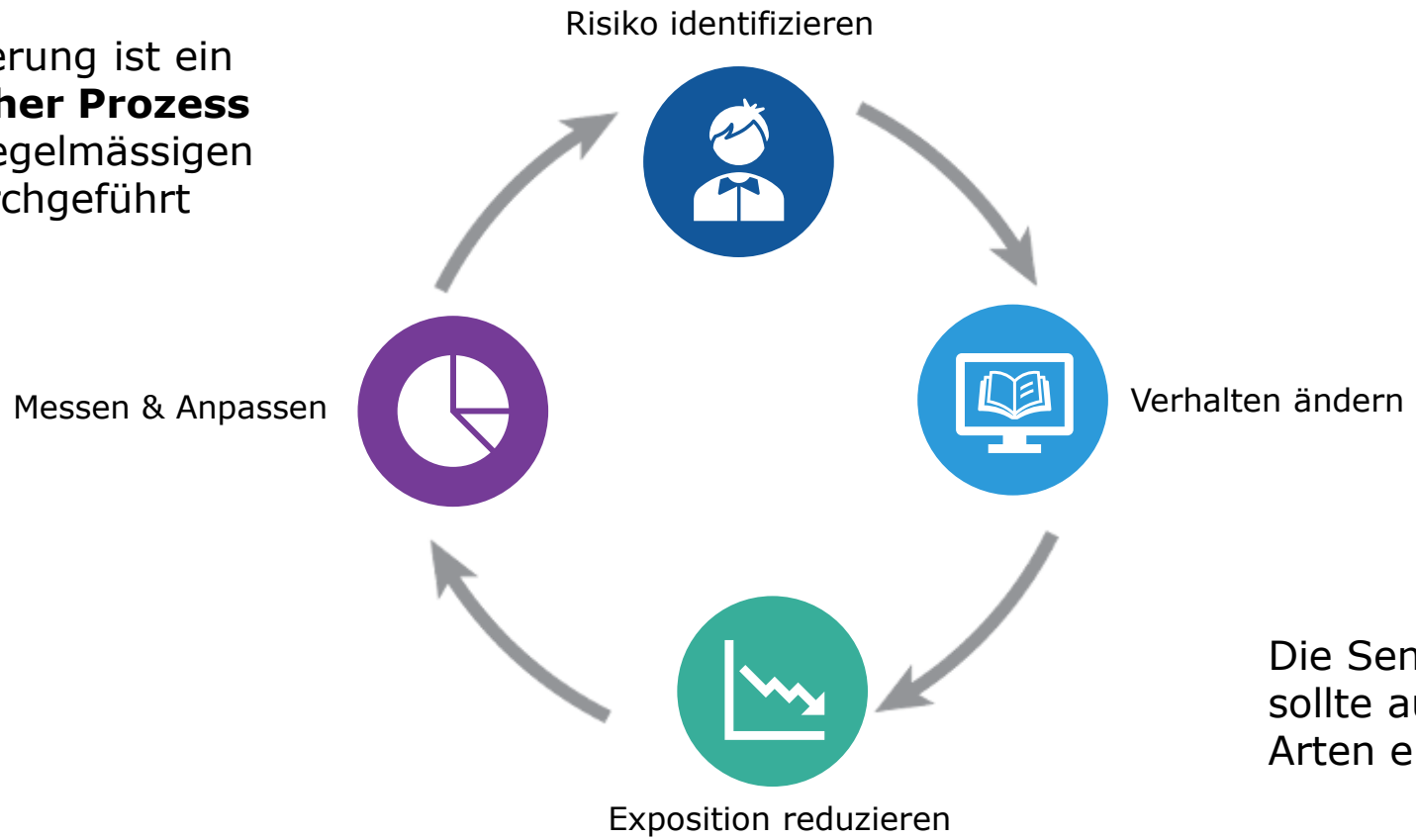
Score = 0 – 1000 Punkte



Security Awareness - Methodologie

Information Security in Healthcare

Die Sensibilisierung ist ein **kontinuierlicher Prozess** und sollte in regelmässigen Abständen durchgeführt werden.



Die Sensibilisierung sollte auf verschiedene Arten erfolgen.

Phishing Themenwahl

Information Security in Healthcare

Häufig verwendete Themen

- Neue Microsoft Teams-Anfragen
- Coronavirus-Alarmmeldungen und Gesundheitswarnungen
- Hinweise zum Ablauf des Microsoft 365-Kennworts
- Deaktivierung eines alten OneDrive-Kontos
- Benachrichtigung über gemeinsamen OneDrive-Vertrag
- Starbucks-Bonus
- Hinweis auf neue Voicemail
- Warnung über die grosse Anzahl von Dateien, die vom OneDrive gelöscht werden

Die raffiniertesten Themen

- Ein Monat kostenloses Netflix Abo für Mitarbeitende
- Vertrag für Ferienvermietung
- Ticketvorverkauf für die Olympischen Sommerspiele
- Benachrichtigung überfällige Rechnungen
- Aufforderung zur Aktualisierung des Spotify-Kennworts
- Schuldschein
- Verletzung der Kleiderordnung
- Coronavirus Maskenverfügbarkeit
- Mitteilung über einen Verkehrsverstoss

Erfahrungsgemäss liegt die Fehlerquote für die raffinierten Themen sehr hoch.

Ergebnisse der Kampagne - Generell

Information Security in Healthcare

Rückmeldung unseres Partners, dessen Kunden 60 Millionen Phishing-Tests in 2020 durchgeführt haben:
Das Thema Unternehmen hat weiterhin Priorität.

Ergebnisse:

→ Durchschnittliche Fehlerquote lag nur bei 11%

→ Abteilungen, die häufiger mit E-Mail zu tun haben, schnitten besser ab

Angreifer sind sich dessen bewusst und gehen wie folgt damit um:

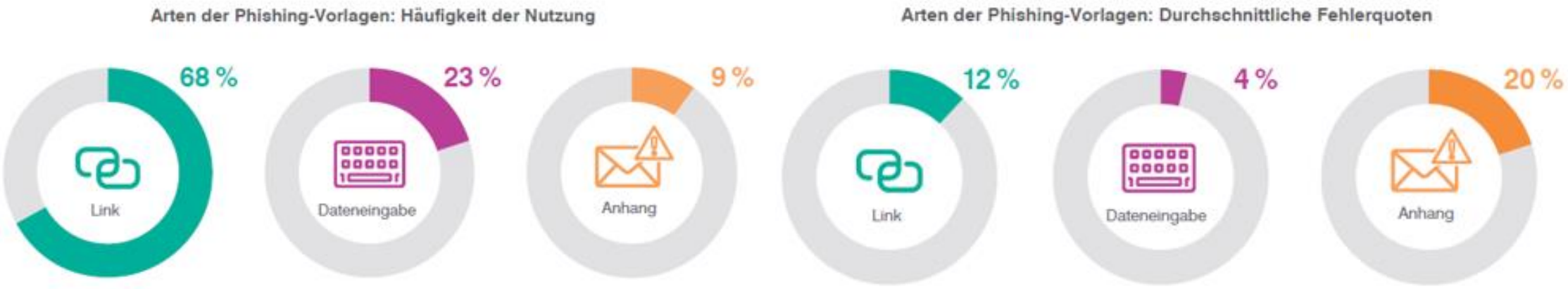
→ Köder werden regelmässig ausgetauscht
- Immer neue Themen
- Art der E-Mail (Links, Dateneingaben, Anhänge)
- Darstellung

→ In einem uns bekannten Case, erfolgte erst ein Telefonanruf, bei dem die E-Mail angekündigt wurde.

Ergebnisse der Kampagne – Aufgrund der Vorlage

Information Security in Healthcare

Aus der gleichen Datenquelle ergab sich folgendes Ergebnis:



"Nicht bestandene" Dateneingabetests beziehen sich auf Fälle, bei denen Anwender nach dem Klick auf einen Link im simulierten Angriff Daten übermittelten.

Was sollte ein Schulungs-Tool beinhalten?

Information Security in Healthcare

ThreatSim® Simulated Attacks

Knowledge Assessments

End User Reporting

Security Awareness Materials

- Simulated Phishing Attacks
- Simulated USB Attacks
- Simulated Smishing Attacks
- CyberStrength®
- PhishAlarm®
- PhishAlarm Analyzer
- Educational Materials
- Awareness Video Campaigns

Security Education Platform

Vollständig integrierte Plattform mit Bewertungen, Schulungen, Berichten und Verwaltungsfunktionen

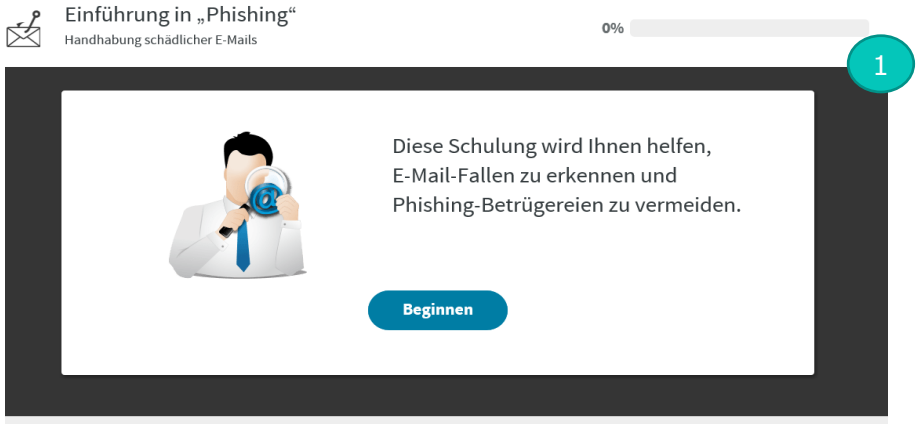
- Bewerten
- Schulung
- Verstärken
- Massnahmen

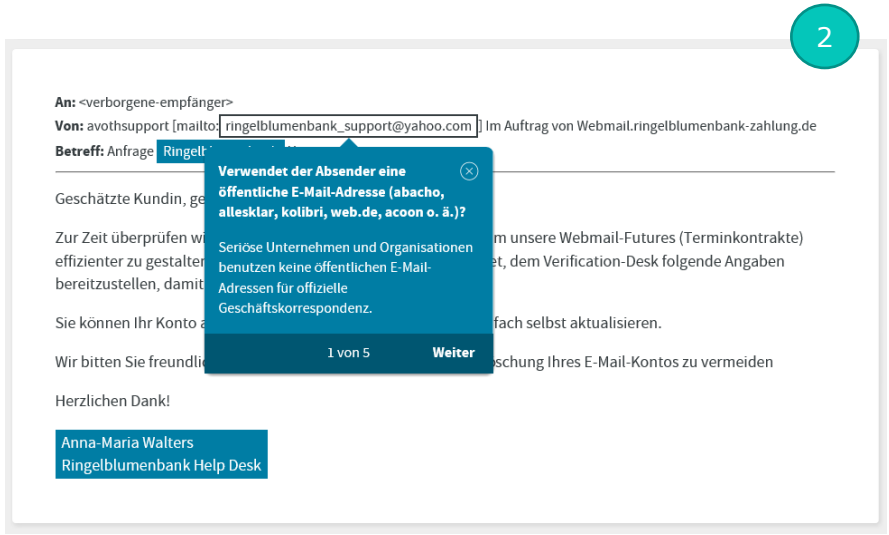
Interactive Training Modules

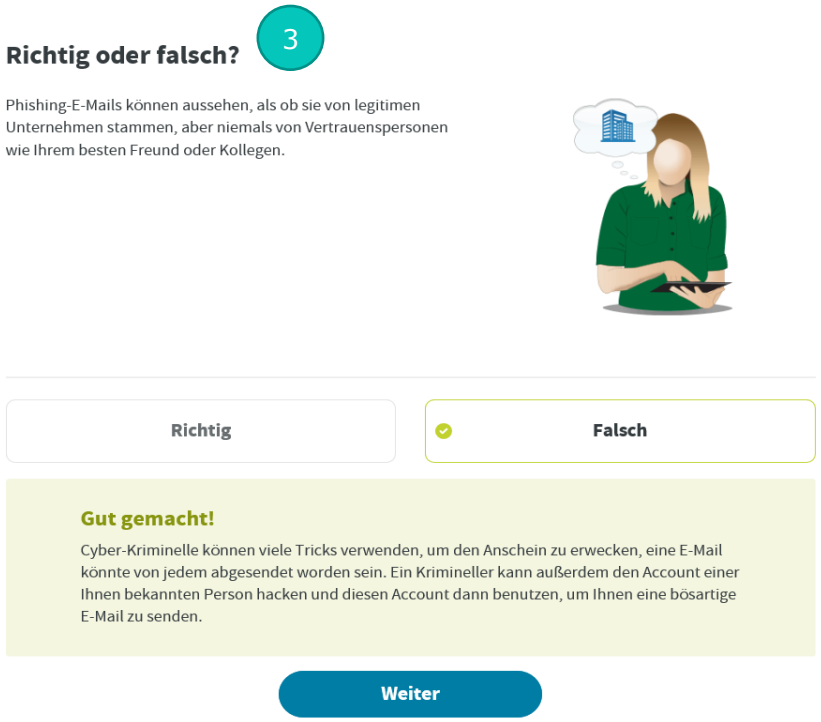
- Safer Web Browsing
- Mobile App Security
- Securing your Email Series
- URL Training
- Social Engineering
- Safe Social Networking
- Physical Security
- Insider Threat Series
- Protecting Against Ransomware
- Travel Security
- Data Protection and Destruction
- Mobile Device Security
- Security Beyond the Office
- Password Protection Series
- USB Device Safety
- GDPR In Action
- Email Security
- Security Essentials for Executives
- Security Essentials
- PHI
- PCI DSS
- PII Series
- GDPR Overview
- Preventing Compromise Series
- Workplace Security in Action

Beispiel Auszug aus einem interaktiven Training

Information Security in Healthcare







Zusammenfassung

Zusammenfassung

Information Security in Healthcare

- → Ausgangslage
  - → Es passiert tatsächlich
  - → Cyber-Security ist kein Technik-Produkt
  - → Der Weg des geringsten Widerstands
- → Cyber Threat Landscape
- → Awareness ganz gezielt
  - → Der Mensch wurde zum Perimeter
  - → Die Verteidigung muss sich den Angreifern anpassen
  - → Gesamtheitliches Awareness-Programm aufgrund Ihrer Risiken (VAP)

AVENIQ

Danke! Fragen und Diskussion.

AVENIQ

Clemens Chizzali-Bonfadin
Expert Consultant Cyber Security

T +41 58 411 76 46
E clemens.chizzali-bonfadin@aveniq.ch

Patrick Gürtler
Senior Consultant

T +41 58 201 62 65
E patrick.guertler@aveniq.ch