
Spitäler und digitale Sicherheit
24.09.2019
Vorkehrungen
Zukunft
HOSPITA
Angriffs-vektoren
Bedrohungs-Lage
LOGICARE

# Bedrohungs-Lage

Niemand zweifelt mehr an der aktiven Bedrohung im digitalen Umfeld - auch im **Schweizer Spitalumfeld!**

Wodurch?

Trend?

Wer?

# Wodurch?

## Auszug aus dem ENISA Landscape Report 2018 (Januar 2019)

Die Bedrohung ist und bleibt aktiv! Neue kommen dauernd dazu, nur sehr wenige verschwinden wieder.

| Top Threats 2017 | Assessed Trends 2017 | Top Threats 2018 | Assessed Trends 2018 | Change in ranking |
|---|---|---|---|---|
| 1. Malware | ➲ | 1. Malware | ➲ | → |
| 2. Web Based Attacks | ↑ | 2. Web Based Attacks | ↑ | → |
| 3. Web Application Attacks | ↑ | 3. Web Application Attacks | ➲ | → |
| 4. Phishing | ↑ | 4. Phishing | ↑ | → |
| 5. Spam | ↑ | 5. Denial of Service | ↑ | ↑ |
| 6. Denial of Service | ↑ | 6. Spam | ➲ | ↓ |
| 7. Ransomware | ↑ | 7. Botnets | ↑ | ↑ |
| 8. Botnets | ↑ | 8. Data Breaches | ↑ | ↑ |
| 9. Insider threat | ➲ | 9. Insider Threat | ↓ | → |
| 10. Physical manipulation/ damage/ theft/loss | ➲ | 10. Physical manipulation/ damage/ theft/loss | ➲ | → |
| 11. Data Breaches | ↑ | 11. Information Leakage | ↑ | ↑ |
| 12. Identity Theft | ↑ | 12. Identity Theft | ↑ | → |
| 13. Information Leakage | ↑ | 13. Cryptojacking | ↑ | NEW |
| 14. Exploit Kits | ↓ | 14. Ransomware | ↓ | ↓ |
| 15. Cyber Espionage | ↑ | 15. Cyber Espionage | ↓ | → |

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

# Trend

## Top 4 Positionen sind 2017 / 2018 unverändert

1


2


3

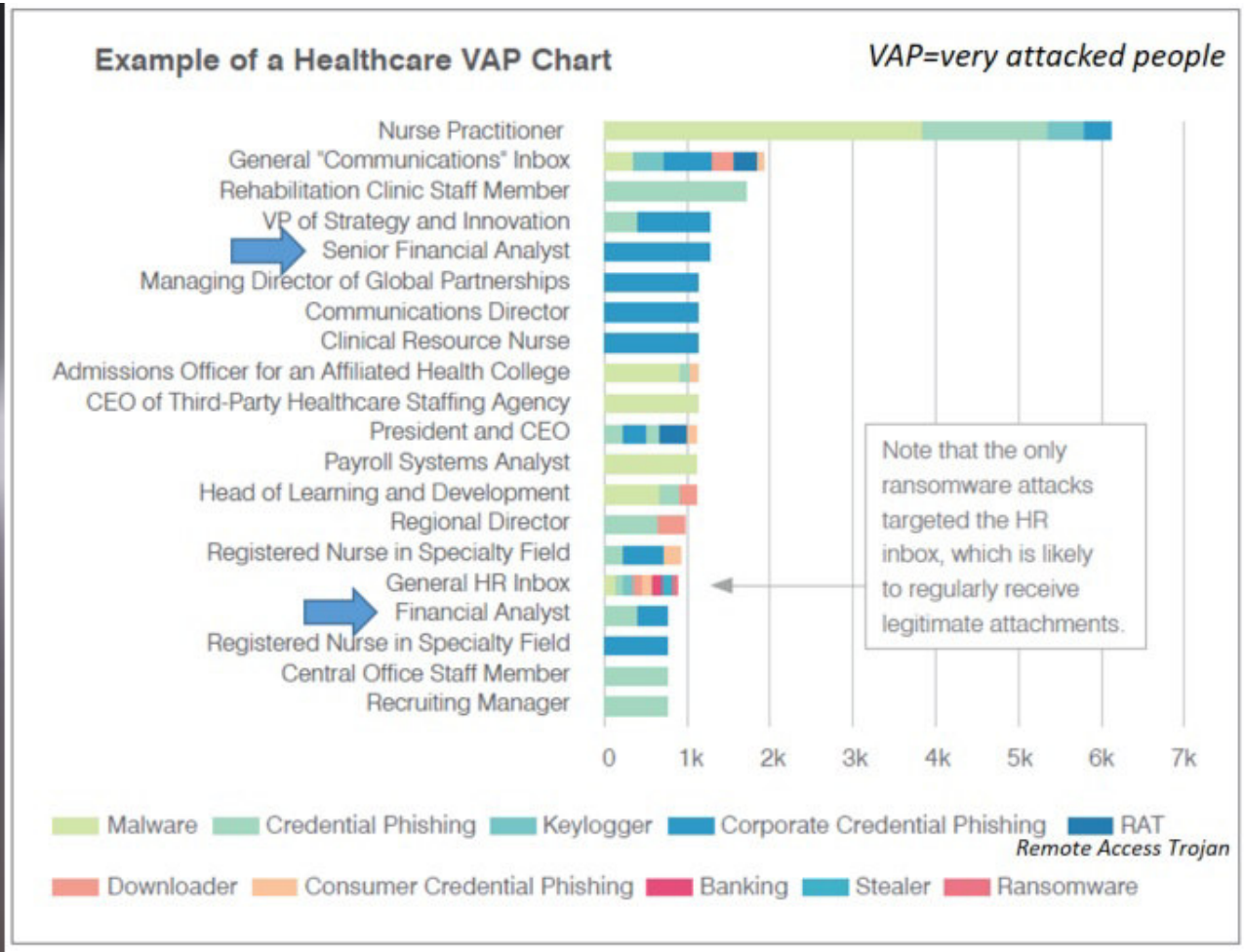

Die Erfassung, Verarbeitung, Speicherung und Übermittlung sensibler Daten – dazu gehören persönliche Daten oder Zahlungsdaten – über **Web-Applikationen** machen diese zum interessanten Ziel für Cyberkriminelle. Dabei spielen Sicherheitslücken in den Web Applikation eine Rolle, die etwa auf kleinere Fehler in der Codierung zurückzuführen sind. Diese Schwachstellen ermöglichen Hackern den direkten Zugriff auf Datenbanken, um sensible Daten zu manipulieren bzw. zu stehlen.


Cryptojacking ist definiert als die unauthorisierte Verwendung Ihres Computers zum Minen von Kryptowährungen. Kurz gesagt wird ein Programm installiert, welches heimlich Kryptowährungen mined. Kryptowährungs-Malware-Angriffe bewirken extrem hohe CPU-Verarbeitung und Netzwerkbandbreitenverbrauch, welche die Stabilität und Verfügbarkeit der physischen Prozesse eines kritischen Infrastrukturbetreibers gefährden können.

4

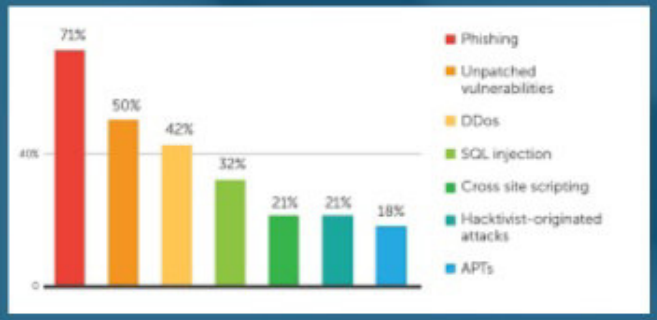
# Wer?


Viele Bedrohungen kommen
aus dem Benutzer-Kontext!




Auswertung von Proofpoint© überwachten eMail-Inboxen eines US-Healthcare-Providers im Jahre 2018 während 3 Monaten.

Als **Angriffsvektor** wird die Kombination von Angriffsweg und -technik bezeichnet, mit der sich ein Angreifer Zugang zu IT- Systemen verschafft.



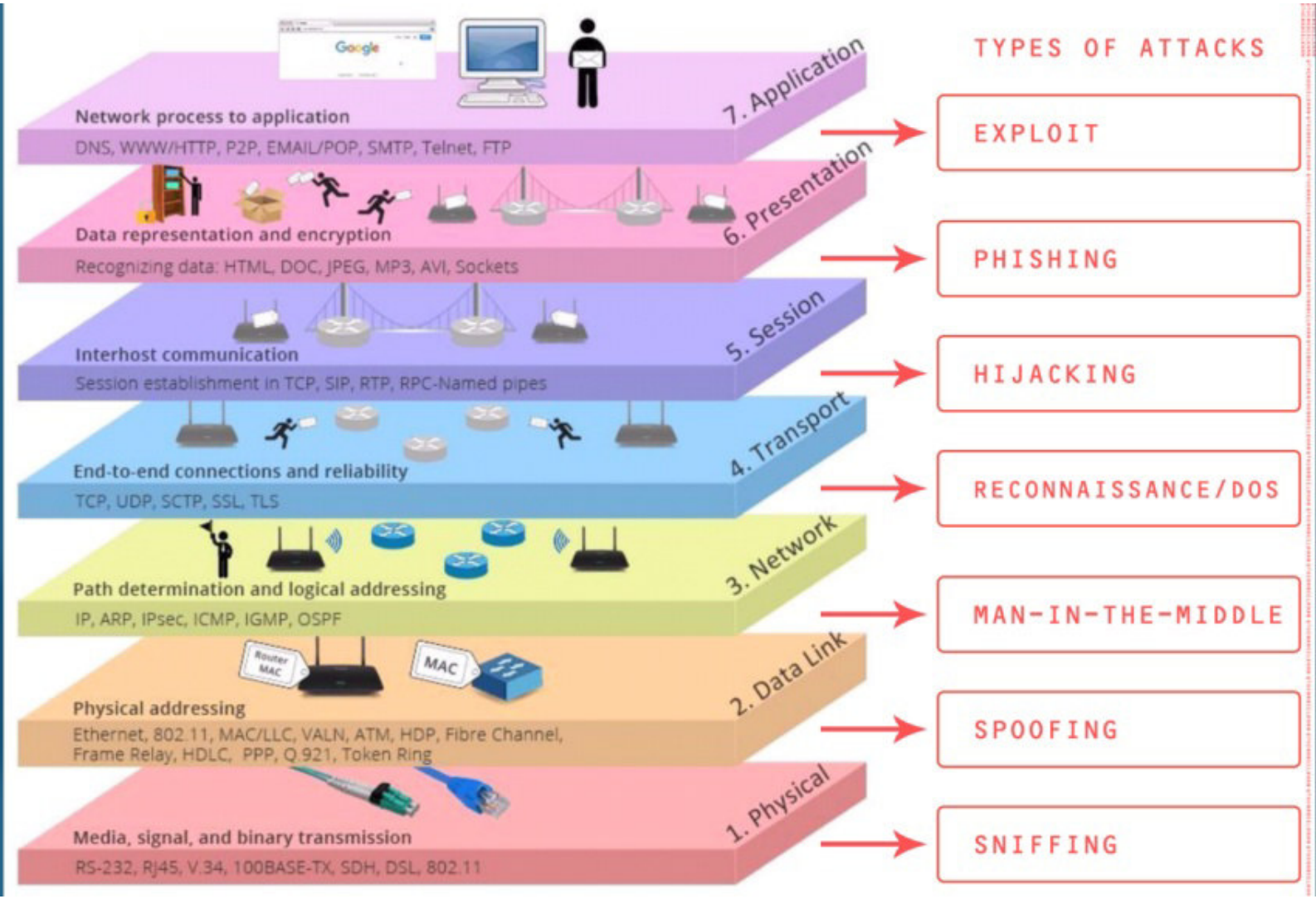

Über raffiniertes "social engineering" (soziale Manipulation) unterstützt von immer neuen Techniken (Phishing, Smishing, Vishing, etc.) werden wir zum leichten Opfer - **oft auch unbemerkt**!

Szenario 1

Szenario 2

Szenario 3

## Angriffsvektoren und Beispiele im CH-Gesundheitswesen


TYPES OF ATTACKS
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
EXPLOIT
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
PHISHING
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
HIJACKING
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
RECONNAISSANCE/DOS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
MAN-IN-THE-MIDDLE
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
SPOOFING
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
SNIFFING

# Szenario 1

**Verschlüsselung oder Löschung von Daten**

**Die Folgen**

- Die benötigten Daten sind nicht verfügbar
- Störung des Arbeitsbetriebs bis zu Spital-Schliessungen aus Behandlungsrisiken

**Reaktionen/Gegenmassnahmen**

- Rekonstruktion der Daten (Backup)
- Bezahlen (nicht empfohlen)

# Szenario 2

**Person oder Partei hat Zugriff auf die Berechtigungen/Daten**

**Die Folgen**

- Interne Informationen werden verbreitet
- Informationen werden verfälscht, falsche Entscheidungen werden getroffen
- Betriebsgeheimnisse werde öffentlich

**Reaktionen/Gegenmassnahmen**

- Hoffen ... (die Informationen können nicht zurück geholt werden!)

# Szenario 3

**Reputationsschaden bei Bekanntwerden eines Vorfalls**


**Die Folgen**

- Die Professionalität / Qualität des Spitals wird in Frage gestellt
- Ungerechtfertigte "Shitstorm"-Attacken
- Patienten wähen anderes Spital --> Vertrauen

**Reaktionen/Gegenmassnahmen**

- PR-Gegenkampagne
- Aussitzen...

# Vorkehrungen und Massnahmen

## Minimalstandard gemäss MELANI

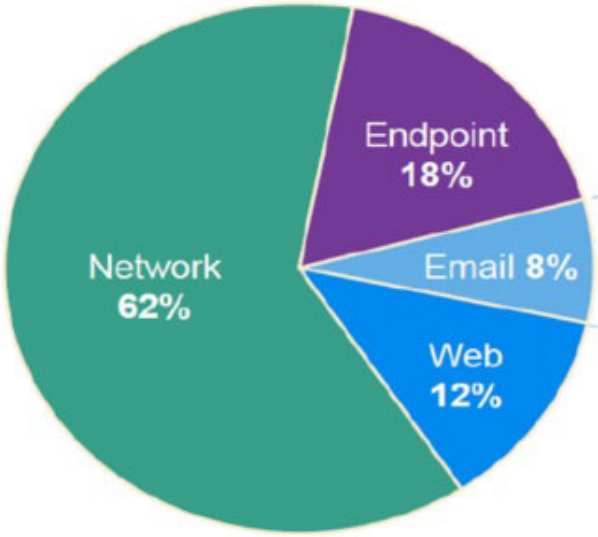
- Schwachstellenanalyse / Assessment
- Sicherheitsstrategie erstellen / umsetzen
- Partner- und Lösungen evaluieren
- Kontrollen definieren und prüfen
- **Mitarbeiter schulen und sensibilisieren**
- Lieferanten und Partner einbinden

| | |
|---|---|
| Risk Management Programm | • Identifizierung von Sicherheitsrisiken<br>• Risikoprofil<br>• Akkurate Bestandsverwaltung der IKT-Betriebsmittel |
| Cybersecurity-Architektur | • Standards/Empfehlungen<br>• Richtlinien<br>• Vorgehensweise |
| Physische Sicherheit | • Schutz von Endgeräten<br>• Kontrollzentrum, Zugangskontrollen<br>• Videoüberwachung, Zugangskontrollen & Barrieren |
| Netzwerk-Architektur | • Typische Sicherheitszonen<br>• Demilitarized Zones (DMZ)<br>• Virtual LANs |
| Netzwerk Perimeter Security | • Firewalls<br>• Fernzugriff & Authentifizierung<br>• Jump Servers/Hosts |
| Host Security | • Patch- & Schwachstellen-Management<br>• Endgeräte<br>• Virtuelle Geräte |
| Security Überwachung | • Intrusion Detection Systems<br>• Sicherheits-Audit-Logging<br>• Sicherheitsvorfall und Event-Überwachung |
| Vendor Management | • Lieferketten Überwachung & Management<br>• Managed Services & Outsourcing<br>• Nutzung von Cloud-Diensten |
| Das Element Mensch | • Richtlinien<br>• Vorgehensweisen<br>• Training und Wahrnehmung |

# IT-Security Awareness Training

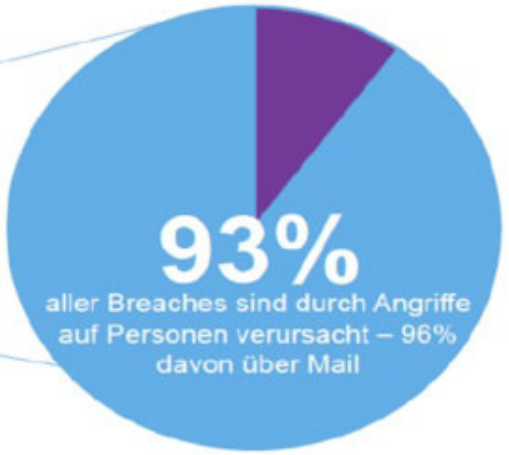
asecus
securing your business

## IT Sicherheitsindustrie



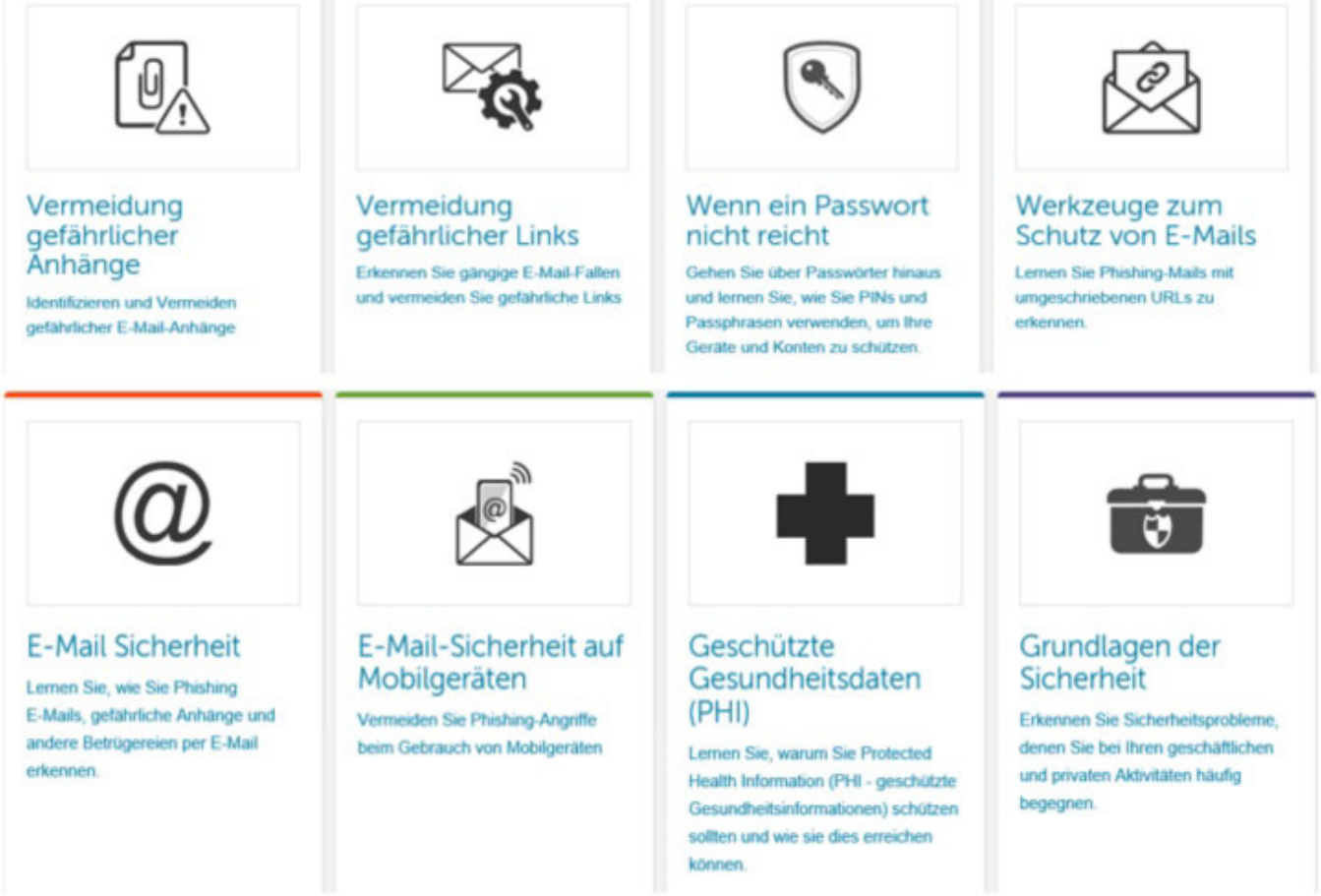

Source: Gartner (2017 forecast)

## Angriffsvektoren

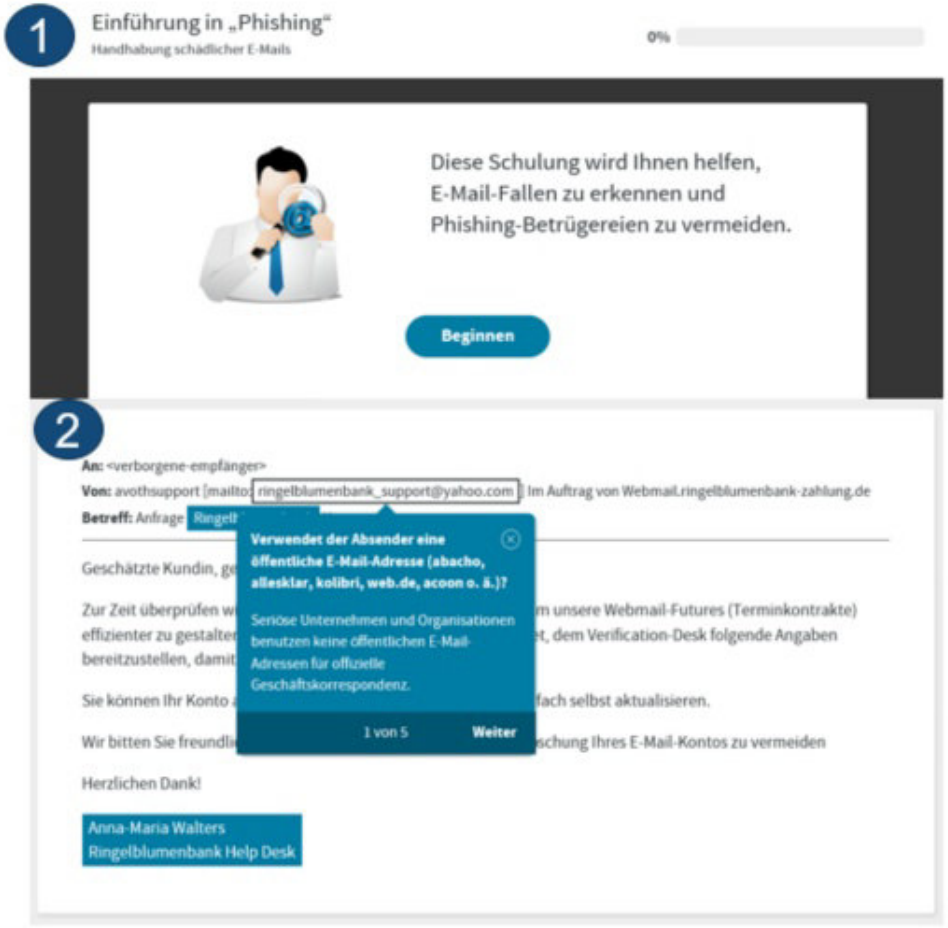



Source: 2018 Verizon DBIR

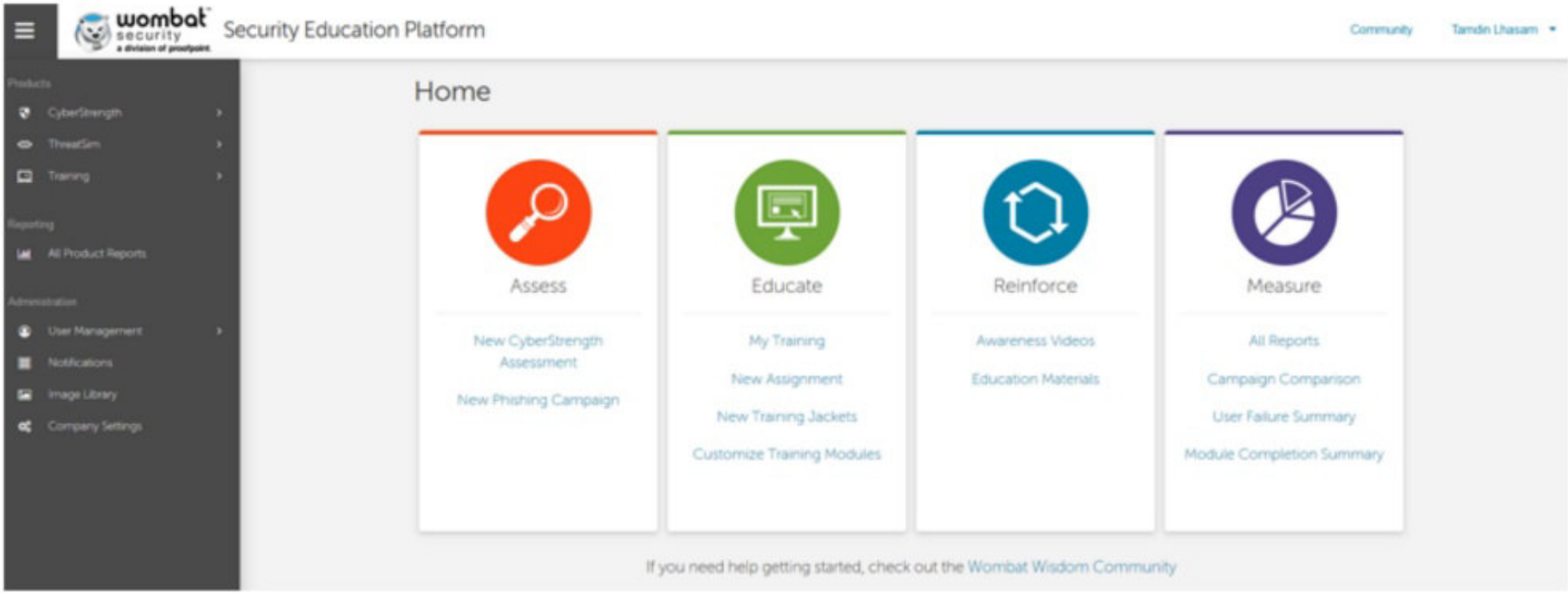
# Themengebiete (Auszug) - Email



# Beispiel Schulung Email




# Security Education Platform




→ Alle Funktionen sind zentral in einer Plattform verfügbar.

# Zukunft

Welche Risiken bringen die Zukunftstechnologien?

AI / KI

Hybrid Cloud

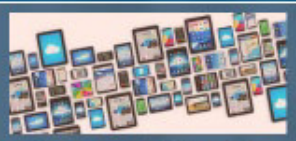
- wer stellt Security sicher?
- wer ist verantwortlich?
- welche Zugriffe/Zugänge sind nötig?

Digitalisierung

Datenhaltung

- wer hat den Schlüssel zu den Daten?
- wer sammelt die Schlüssel wieder ein?

Mobiliät



- sind alle Geräte geschützt?
- wo sind die Daten überall gespeichert?


Sicherheit
Risiko
Was können SIE zur digitalen Sicherheit im Spital beitragen?
• Machen Sie Sicherheit / Datenschutz zum dauernden **Management-Thema**
• **Sensibilisieren** Sie durch "Angriffe", **Training** und ständige Kommunikation ihre Mitarbeitenden
• Lassen Sie sich die bestehenden technischen Schwachstellen in ihrer Umgebung aufzeigen (die gibt es überall!!) und entscheiden Sie bewusst, welche Risiken ihr Spital tragen will oder wo geeignete **Massnahmen** oder **Versicherungen** evaluiert werden sollen. Lassen sie diese Entscheidung vom obersten Führungsorgan sanktionieren!
• **Seien Sie bereit** - es wird passieren... (Notfallplan!)

# Viel Erfolg!

LOGICARE


Spitäler und digitale Sicherheit
24.09.2019
Vorkehrungen
Zukunft
Angriffs-vektoren
Bedrohungs-Lage
LOGICARE