meier tobler

Cyberattacke auf den Haustechniker Meier Tobler

Martin Schäppi
Leiter Unternehmenskommunikation
November 2020

Agenda

1. Profil Meier Tobler AG
2. Cyberangriff 24.07.19
3. Konsequenzen und Lehren
4. Ihre Fragen

Unser Geschäft

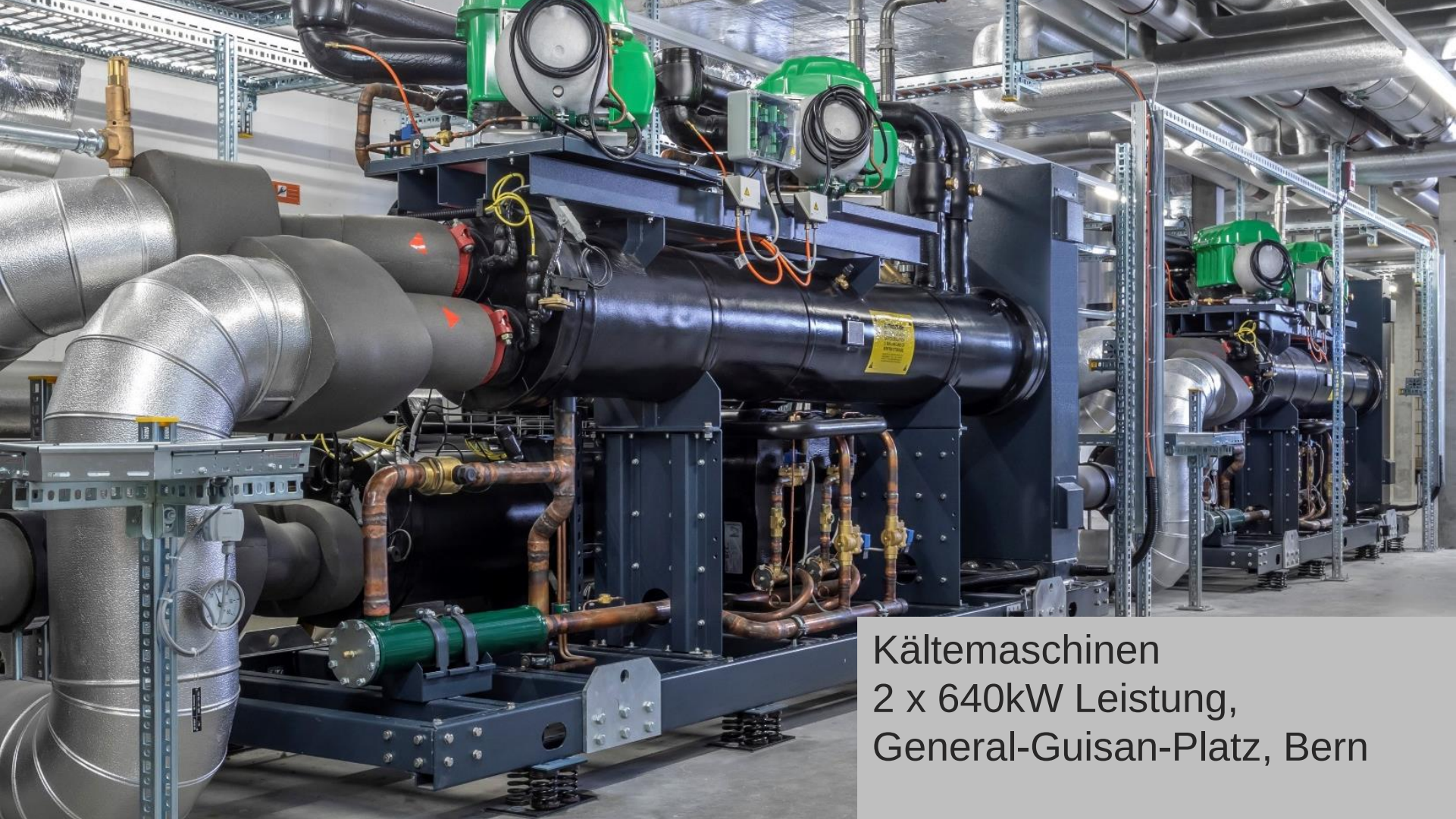
meier tobler

«Einfach Haustechnik»

1304 Mitarbeitende, CHF 496 Mio. Umsatz, CHF 27 Mio. EBITDA				2019
Handel 	Wärmeerzeugung 	Service 	Klimasysteme 	Bereiche
10’000 Installateure		260’000 Liegenschafts-besitzer	Installateure, Bauherren	Kunden/ Partner

Service und Werterhalt,
24h/365, schweizweit,
on-site und remote

Inspektion, Messung und Reinigung von Lüftungs- und Reinraumanlagen



Kältemaschinen
2 x 640kW Leistung,
General-Guisan-Platz, Bern

Photovoltaik plus Wärmepumpe,
EFH Illnau-Effretikon


Wärmepumpe
Brauchwarmwasser-Speicher
Heizwasser-Speicher

Wechselrichter

Batterie

Energie-Manager

Der jüngste Marché in Bulle:
Eröffnet im Mai 2019

Agenda

1. Profil Meier Tobler AG
2. Cyberangriff 24.07.19
3. Konsequenzen und Lehren
4. Ihre Fragen

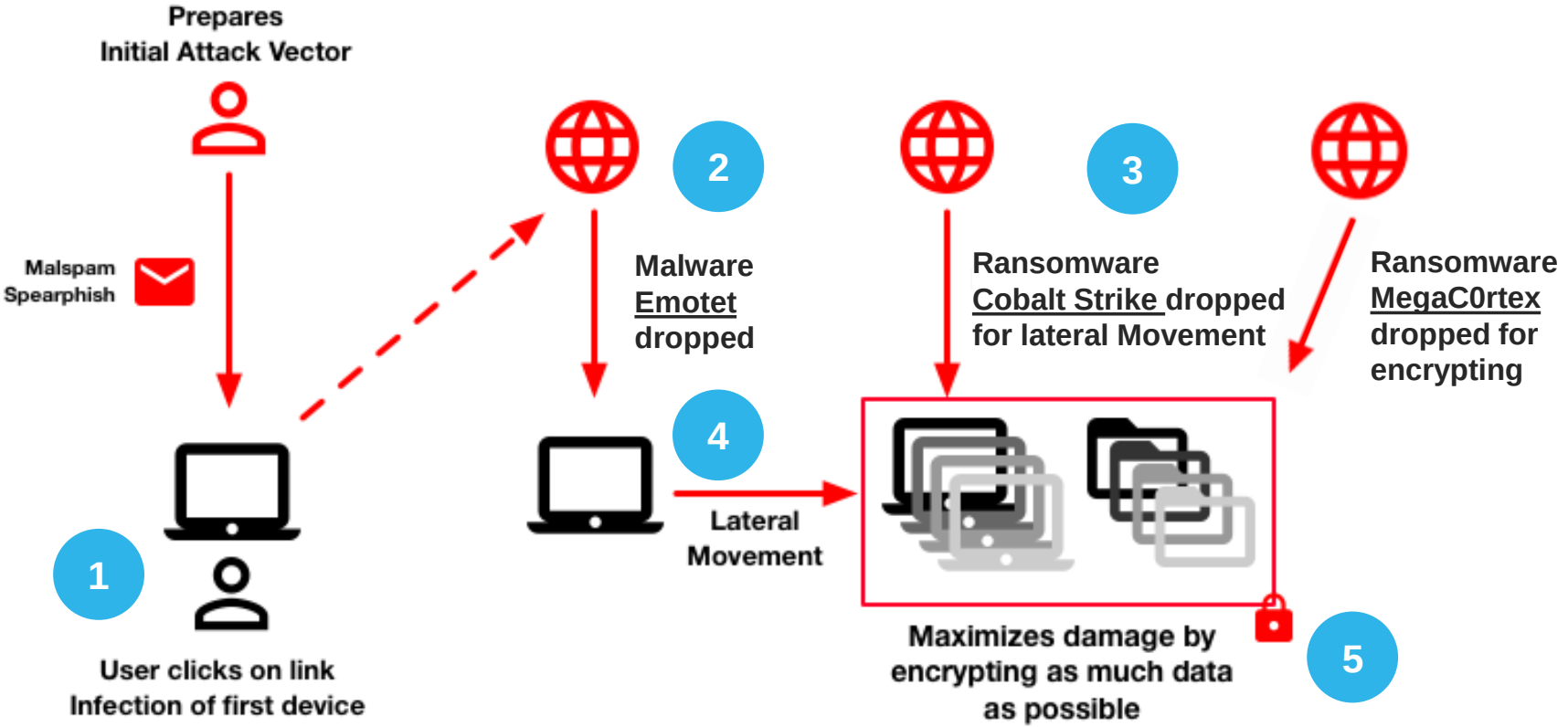
Cyberangriff 24. Juli

meier tobler

Link auf Video:
https://vimeo.com/352427866/9c4d525a67?utm_content=CEOnewsletter%20%E2%80%93%20August%202019%20-%20DE

Ablauf Cyberangriff

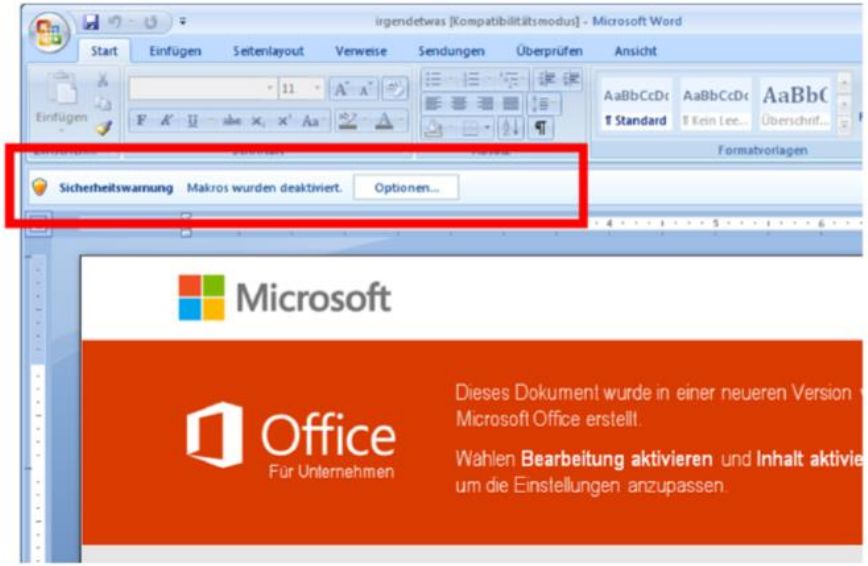
meier tobler



1 Malspam: Anhang aktiviert Emotet

meier tobler

- Dokument öffnet sich im geschützten Modus
- Empfänger aktiviert Bearbeitung
- im Hintergrund startet Makro
- Makro lädt Emotet-Malware
- Mai 2019



Quelle: InfoGuard

2 Angriffs-Werkzeug Emotet

- Seit 2014 bekannt
- Etabliert Initialzugang für Verkauf im Darknet
- Ermöglich Nachladen anderer Malware
- Schwer erkennbar, mutiert im Wochentakt
- Ab April 2019 werden echte E-Mails verändert und genutzt
- «Dynamit Phishing»

Quelle: InfoGuard

3 4 Angriffs-Werkzeug: Cobalt Strike

- Werkzeugkasten und Operationsbasis für Angriff
- Erlaubt die Ausbreitung im Netz

5 Angriffs-Werkzeug: MegaC0rtext

- Verschlüsselungs-Software

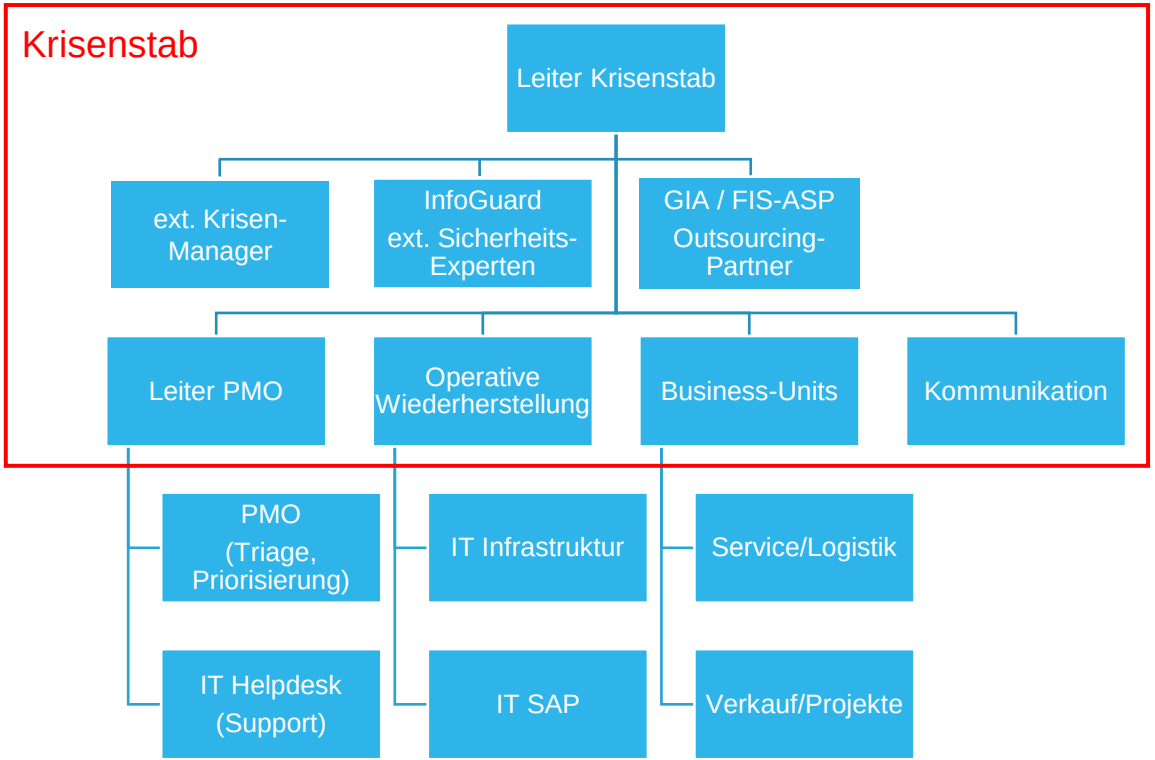
Quelle: InfoGuard

Chronologie Cyberangriff 24.07.19

meier tobler

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

Krisenorganisation



- Regelmässige Rapporte (08:00, 11:00, 14:00, 17:00)
- Arbeitszeit 7x24h
- Ablösung und Stellvertretung

Agenda

1. Profil Meier Tobler AG
2. Cyberangriff 24.07.19
3. Konsequenzen und Lehren
4. Ihre Fragen

Erkenntnisse

- Neue Dimension der Cyberangriffe erreicht: «Dynamit Phishing»
- Organisiertes Verbrechen betreibt Arbeitsteilung
- Kombination opportunistischer und gezielter Attacken
- Alle sind betroffen, unabhängig der Grösse
- Frage des Aufwands, den die Angreifer betreiben wollen
- Beim Angriff ist Mensch schwächstes Glied (Social Engineering)
- Bei Bewältigung des Angriffs ist der Mensch das stärkste Element

- **Klassische Sicherheits-Vorkehrungen reichen nicht mehr**

Cybersicherheit Struktur

meier tobler

Identifi-zieren	Schützen	Erkennen	Reagieren	Wieder-herstellen
Inventur-Mgmt	Zugriffs-Mgmt	Vorfälle	Response-Planung	Wiederherstellung-Planung
Geschäftsumfeld	Zugriffs-Steuerung	Überwachung	Kommunikation	Verbesserungen
Governance	Bewusstseins-Training	Detektions-Prozesse	Analyse	Kommunikation
Risiko-Mgmt	Datensicherheit		Linderung	
Risiko-Mgmt-Strategie	Unterhalt		Verbesserungen	
	Schutztechnologie			

Lehren daraus, technisch

meier tobler

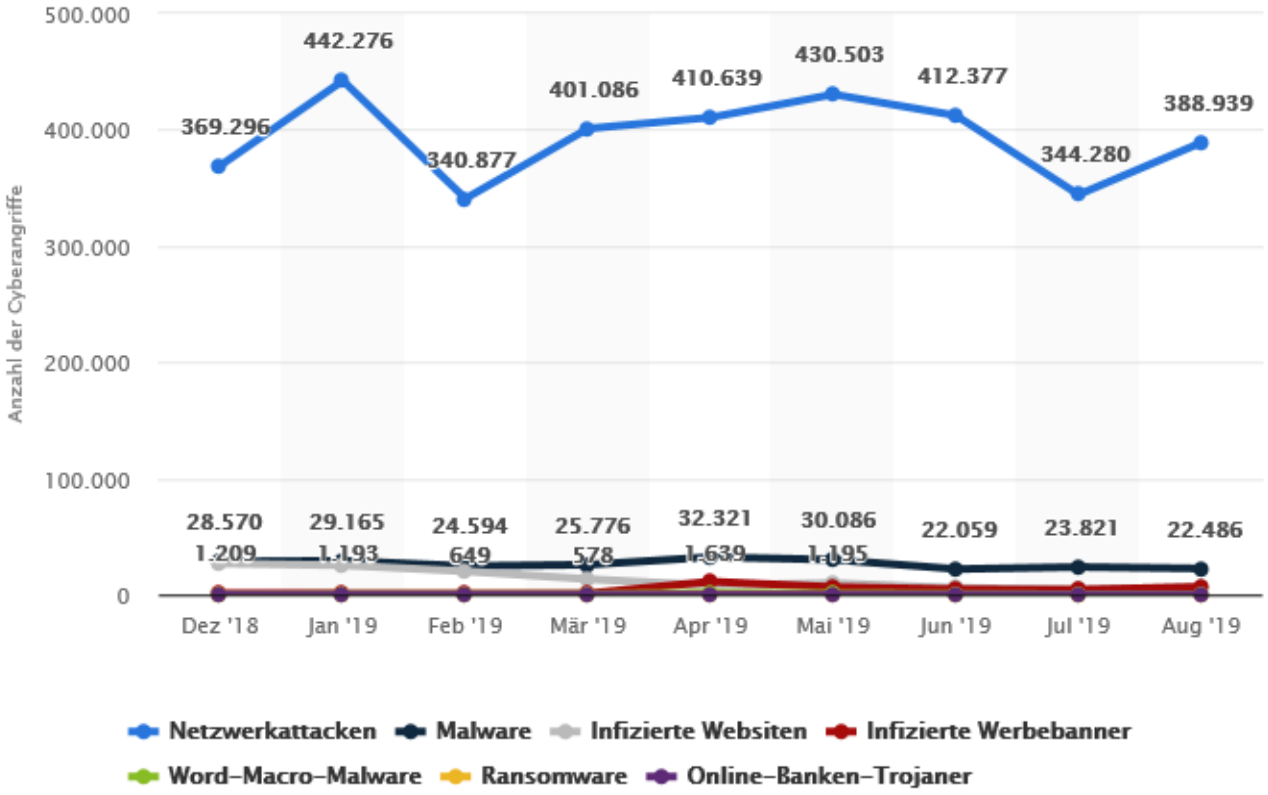
- Zusätzliche Sicherheitsmassnahmen
- Verschärfung Policies (Anhänge E-Mail, Whitelisting Websites, Makros)
- Einführung Zwei-Faktor-Authentifizierung
- Einführung 7x24h aktive Überwachung der Systeme (Tanium)
- Sandboxen zur Abklärung potenziell gefährlicher E-Mails
- Unterteilung Netzwerk in mehrere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

Lehren daraus, organisatorisch

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

Bedrohungslage

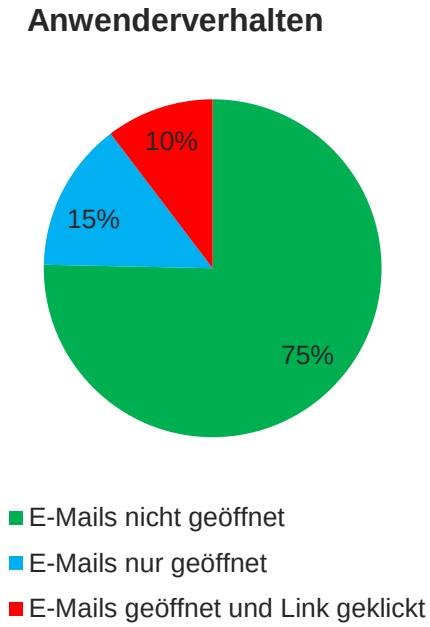
Registrierte Cyber-Angriffe CH



Quelle:
https://de.statista.com/statistik/daten/studie/73932/umfrage/anzahl-registrierter-cyberangriffe-pro-monat-in-der-schweiz/

Faktor Mensch: Sensibilisierungskampagne Juni 2018

- Rund 1200 Anwender wurden mit fünf simulierten, personalisierten E-Mails aus 12 Vorlagen kontaktiert
- Auswertung der Reaktionen der Anwender
- Aufklärung der Anwender die einen Link klickten mittels interaktivem E-Learning



Faktor Mensch: Spear-/Dynamit-Phishing

meier tobler

- Erzeugt Gefühl der Dringlichkeit
- Nutzt vertrauenswürdige Absender
- Verwendet betriebsübliche Betreffzeilen
- Weckt die natürliche Neugier und missbraucht sie
- Nutzt eingeprägte Reaktionen auf häufige und normale Ereignisse (wie beispielsweise Software-Updates)
- Kopiert echte E-Mail als Basis für Fälschungen
- Passt sich der Firmenkultur an (beispielsweise Du-/Sie-Form)

meier tobler

Ich freue mich auf Ihre Fragen!

meier tobler

Alle Infos:
meiertobler.ch

Danke für Ihre Aufmerksamkeit.