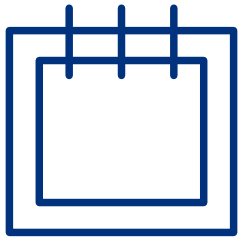
Der Mensch als Sensor

Konferenz@Temet, 29. März 2023, Claudio Truttmann
Öffentlich

Einführung



- Set the Stage..
- Angriffsvektor «E-Mail»
- Integriertes Verhaltensmodell
- Aus der Praxis bei der CSS
- Keyfaktoren «Mensch als Sensor»

- Claudio Truttmann
- Fach-Circle Lead Security Operations Center (SOC) bei der CSS
- Seit 2016 bei der CSS tätig
- claudio.truttmann@css.ch

Social Engineering

Neue Phishing-Welle erreicht die Schweiz – so wollen die Betrüger übers Ohr hauen

Der Bund warnt: Kriminelle versenden aktuell gefälschte E-Mails im Namen der Schweizerischen Eidgenossenschaft. Sie haben es auf Kreditkartendaten abgesehen. Auch Fake-Anrufe im Namen des BAG sorgen für

MFA Fatigue: Hackers' new favorite tactic in high-profile breaches

Hackers are more frequently using social engineering attacks to gain access to corporate credentials and breach large networks. One component of these attacks that is becoming more popular with the rise of multi-factor authentication is a technique called MFA Fatigue.

LAWRENCE ABRAMS SEPTEMBER 20, 2022 06:30 AM 1

Vishing cases reach all time high

Help Net Security May 24, 2022

Vishing (voice phishing) cases have increased almost 550 percent over the last twelve mo 2022 to Q1 2021), according to the latest Quarterly Threat Report from Agari and PhishLabs.

BEC Attacks Surge 81% in 2022

8 FEB 2023 NEWS

Phil Muncaster UK / EMEA News Reporter, Infosecurity Magazine

Email Phil Follow @philmuncaster

Recorded business email compromise (BEC) attacks increased by more than 81% during 2022 and by 175% over the past two years, with open rates on malicious emails also surging, according to Abnormal Security.

Home > News > Security > Ransomware gangs move to 'callback' social engineering attacks

Ransomware gangs move to 'callback' social engineering att

By Ionut Ilascu

August 10, 2022 04:45 PM 0

CNET Your guide to a better future

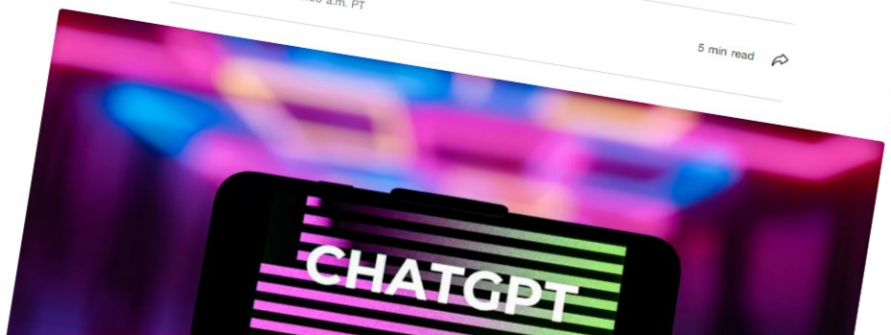
Tech > Services & Software

It's Scary Easy to Use ChatGPT to Write Phishing Emails

I did it as a test -- and I'm worried about how well it worked. I'm not alone in my concerns about the potential use of AI in cyberattacks.

Bree Fowler Feb. 16, 2023 5:00 a.m. PT

5 min read



UK > Software & Services > Security > Password Managers

Hacker Breached LastPass by Installing Keylogger on Employee's Home Computer

The hacker also exploited a vulnerability in a 'third-party media software package' to help launch malware on the employee's computer.

by Michael Kan Feb 28, 2023


Faktor Mensch

Angriffsvektor «E-Mail»

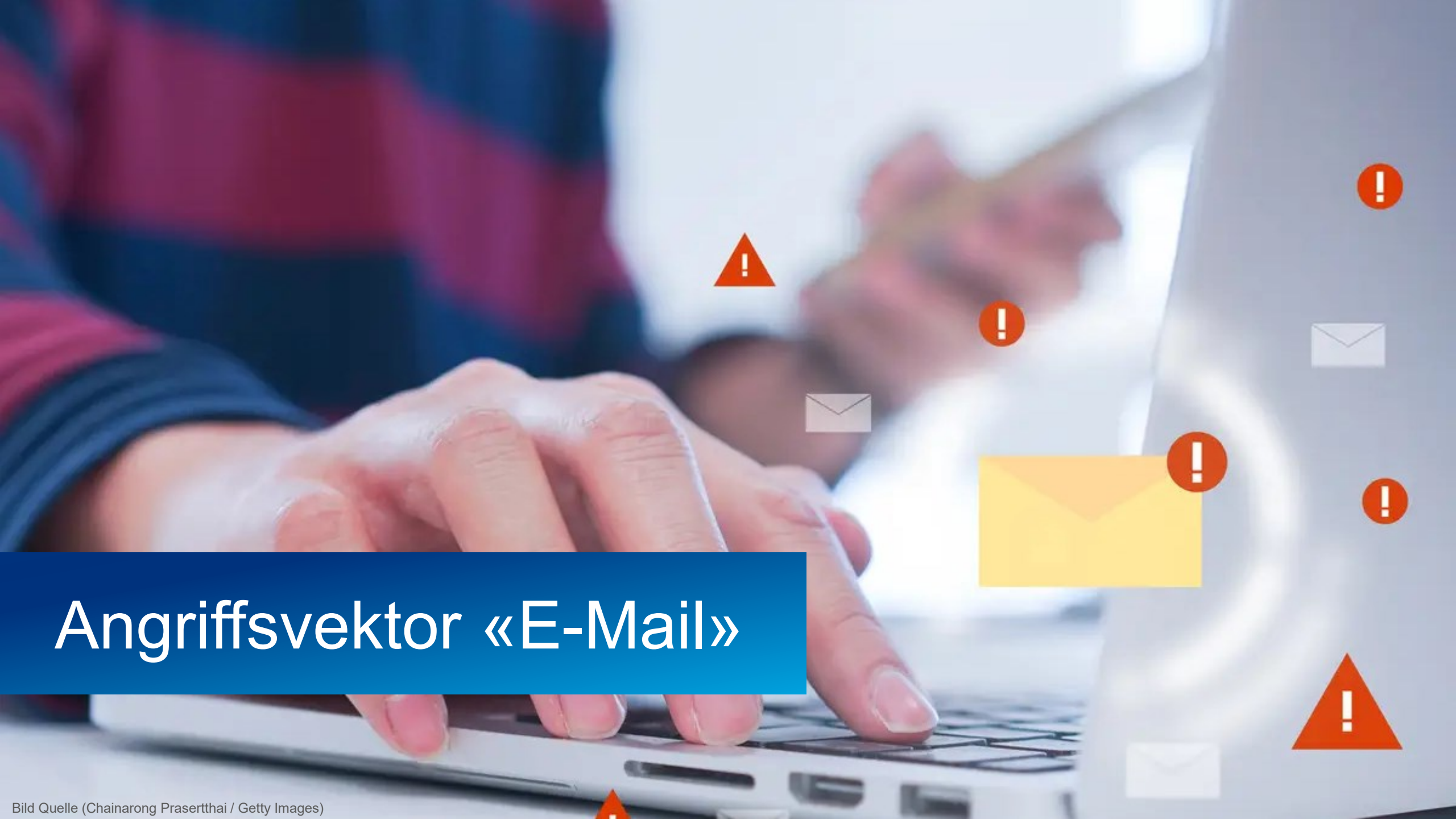
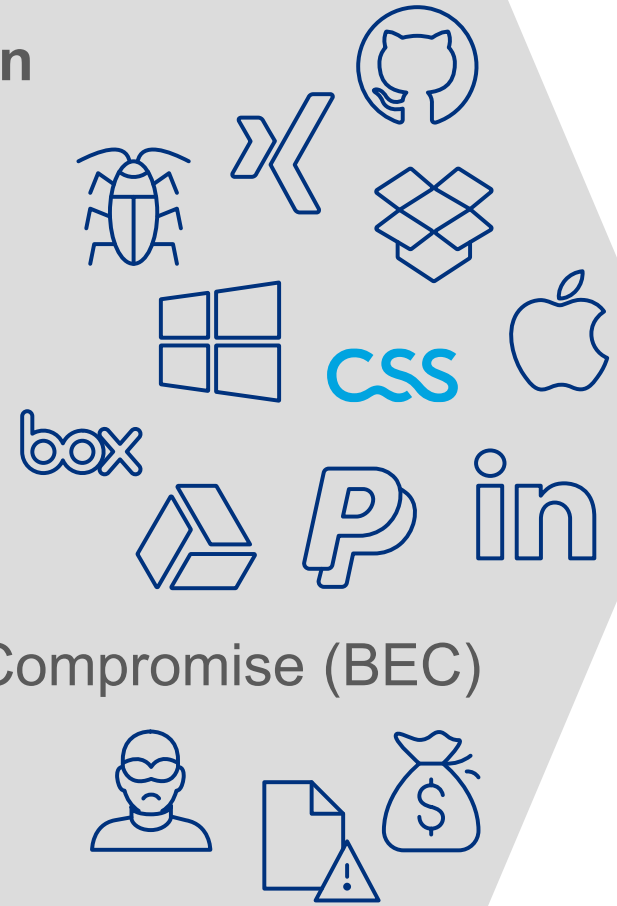


Bild Quelle (Chainarong Prasertthai / Getty Images)

Bedrohungen via E-Mail

E-Mail Bedrohungen

- Phishing
- Spear-Phishing
- Malware
- Fraud / Scam
- Sextortion
- Business E-Mail Compromise (BEC)
- Whaling
- (Spam)



Schutz der Bedrohungen durch

- Technologien
- Prozesse
- Menschen (Verhalten)

Security-Incident Prozess

Identify

- Analyse E-Mail (Sender, URLs, IPs, Anhänge)
- Reputationschecks
- Sandboxing
- Involvierte Accounts
- Abklärung Zeitrahmen
- [illegible]
  - [illegible]
  - Endgeräteaktivitäten
  - Useraktivitäten

Contain

- Blockieren von IPs/Domains/URLs
- Blockieren E-Mail Anhänge
- Blockieren E-Mail Sender
- Blockieren von User-Account
- Blockieren Dateiausführungen auf Application Control

Eradicate

- E-Mails aus Posteingang löschen
- Bösartige Anhänge löschen
- Passwortwechsel initiieren

Recovery

- User-Account reaktivieren
- Entfernen von temporären Regeln

Wie wird der Prozess überhaupt gestartet ?

Technisch (Alarme, Anomalien)

Meldung durch Mitarbeiter

Mitarbeiter Meldeprozess

Prepare | Identify

Meldeprozess ?

- IT-Support-Organisation
- Security-Organisation
- Meldebutton in Mailclient
- Keiner/Undefiniert (z.B. Löschen)
- Technische Meldungen

Zusammenspiel Mitarbeiter und SOC

Mitarbeiter

SOC
(Security-Organisationen)

Was beeinflusst nun das Verhalten der Mitarbeiter ?

Meldung vornehmen

Unterstützung bei Analysen

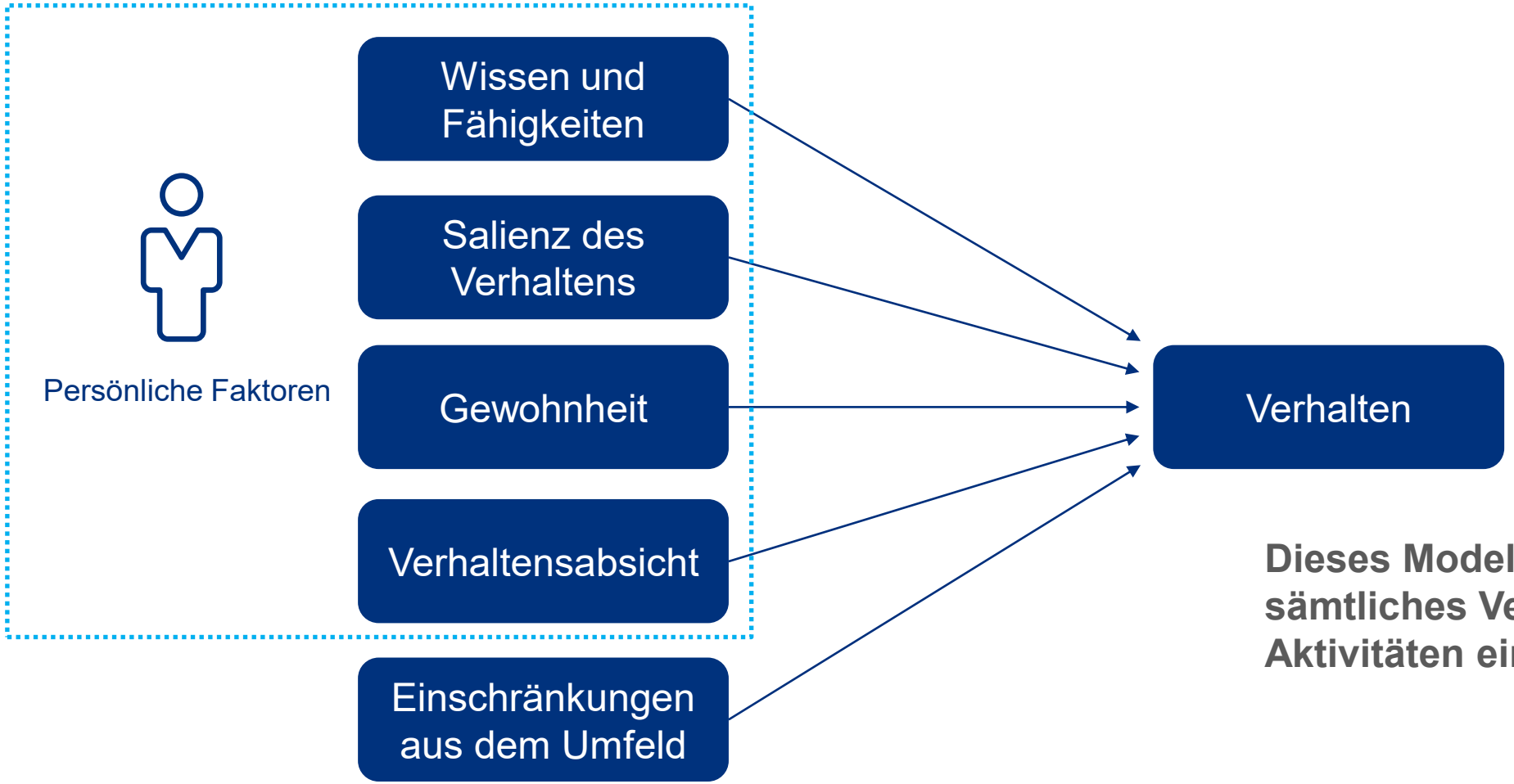
Schaden verhindern oder minimieren

Security Awareness schaffen

Abklärungen mit Mitarbeiter

Integriertes Verhaltensmodell

Das integrierte Verhaltensmodell (vereinfacht)



Dieses Modell gilt natürlich für sämtliches Verhalten aller Aktivitäten eines Menschen!

Angelehnt an das integrierte Verhaltensmodell (IBM) von Montaño und Kasprzyk aus dem Jahre 2008.

Aus der Praxis

Bild Quelle https://latesthackingnews.com/2022/01/29/5-reasons-why-email-is-the-top-attack-vector/

Aus der Praxis bei der CSS (1)

Herausforderungen beim «Menschen als Sensor»

«Dies ist eine E-Mail eines unserer Kunden und wenn ich dieses melde, ist es weg!»

«Änderungen von Bankverbindungen erhalten wir oft über diesen Weg. Warum sollte hier ein Problem sein?»

«Woher und wie hätte ich dieses E-Mail als gefährlich erkennen können?»

«Solche Anhänge habe ich noch nie erhalten, vielleicht verwendet der Kunde eine andere Anwendung mit der er uns etwas zukommen lassen will.»

«Wieder ein Dokument, welches per E-Mail mit mir über einen Cloud Service geteilt wird.»

«Warum kann ich an diesem Gewinnspiel nicht teilnehmen? Wenn ich es mir an die private Adresse sende, funktioniert es aber?»

«Ich stand mit dem Kunden bereits in Kontakt und er hat mir hier noch ein Dokument auf eine bestehende Kundenkommunikation gesendet.»

Aus der Praxis bei der CSS (2)

Anpassung Meldeprozess

Verdächtige E-Mails löschen

- Wenig Visibilität durch die Security-Organisationen im Bereich E-Mail Angriffsvektor.
- Genaues Vorgehen bei verdächtigen E-Mails teilweise zu wenig bekannt bei Mitarbeitern.
- Gemeldete E-Mails wurden teilweise in unterschiedlichen Teams analysiert.

Alle verdächtigen E-Mails melden

- Deutlich höhere Visibilität der verdächtigen E-Mails, welche die verschiedenen E-Mail Schutzmassnahmen umgehen.
- Verbesserte Reaktion aus dem SOC im Bereich des «E-Mail» Angriffvektors.
- Einfacher und schneller Meldeprozess für die Mitarbeiter.
- Mehr Praxisbeispiele für interne Awarenessschulungen, welches die Awareness in diesem Bereich zusätzlich erhöht.
- Gezieltere Awarenessschulungen werden möglich.

Aus der Praxis bei der CSS (3)

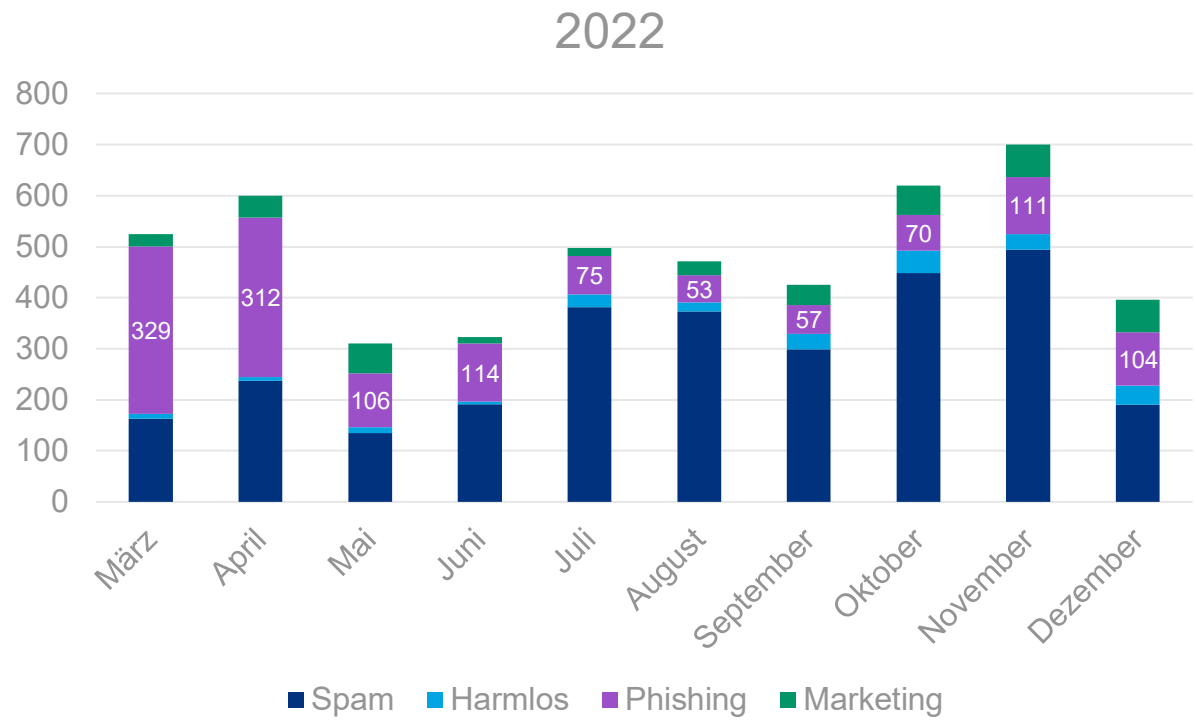
Kennzahlenentwicklung

Verdächtige E-Mails löschen

Total analysierte E-Mails pro Jahr
~ 120

Total identifizierte Phishing E-Mails pro Jahr
~ 40

Alle verdächtigen E-Mails melden



Total durch unseren Partner analysierte E-Mails pro Jahr
4’867

Total identifizierte Phishing E-Mails pro Jahr
1’331

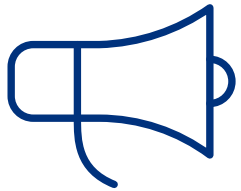
Keyfaktoren damit der «Mensch als Sensor» einen wertvollen Beitrag an die Cybersicherheit im Unternehmen leisten kann

Awareness (Verhalten)

- Alle Mitarbeiter
- Zielgerichtet
- Praktische Beispiele
- Wichtigkeit aufzeigen
- Demonstrationen
- Simulationen

Vertrauen schaffen

- In Bearbeiter
- In Prozess
- Bezug schaffen



Meldeprozess

- Einfach, klar, verständlich
- Schnell
- Wiederverwendbar
- Standardisiert
- Automatisiert

Zusammenarbeit

- Unkompliziert
- Direkt
- Hilfsbereit
- Angriffe entdecken
- Verdächtige Aktivitäten klären
- Angriffe zusammen verhindern

Für die frühzeitige Erkennung von (gezielten) Cyberangriffen ist es essentiell, dass die Zusammenarbeit zwischen den Mitarbeitern und Security-Organisationen einfach, direkt und schnell erfolgen kann.


Dankeschön!

Backupslides

Ausführliches integriertes Verhaltensmodell