Sicherere Mitarbeiter!

Cyber Security Awareness mit LUCY

Swiss eHealth Forum
06. März 2020

Manuel Krucker, manuel.krucker@terreactive.ch
Samuel Flükiger, samuel.fluekiger@mobi.ch

Die Referenten

Manuel Krucker
Cyber Security Consultant
terreActive AG

manuel.krucker@terreactive.ch

Samuel Flükiger
IT-Sicherheitsbeauftragter
Die Mobiliar

samuel.fluekiger@mobi.ch

Agenda

terreActive = security.ch seit 1996. 60 Mitarbeiter, inhabergeführt, SOC in Aarau.

- Ausgangslage
- Weshalb braucht es Cyber Security Awareness?
  - Was ist das Problem?
  - Was sind die Auswirkungen?
  - Welche Massnahmen reduzieren die Risiken?
- Fazit

Ausgangslage

Cyberattacken führen zu komplettem Betriebsausfall

Malware legt mehrere Krankenhäuser in Ostengland lahm

Betroffen ist unter anderem das Diana, Princess of Wales Hospital in (

Wegen einer Infektion der eigenen IT mit Malware m Großbritanniens mehrere Krankenhäuser am Monta weitestgehend einstellen. Die IT-Systeme würden he Problem zu beheben.

November 2016

Fürstenfeldbruck: Malware legt Klinikums-IT komplett lahm

Juli 2019

Im bayerischen Fürstenfeldbruck muss die örtliche Klini komplett ohne Computer auskommen; verantwortlich is

Von **Martin Holland**

Das Klinikum Fürstenfeldbruck (Bild: Klinikum FFB)

November 2018

Zurück zu Bleistift und Papier: Schadsoftware legt Klinikserver lahm

Dezember 2019

Der Albtraum jeder Klinikleitung: Malware legt die Systeme im Kranke lahm. So geschehen ist das in mehr als zehn Häusern in Rheinland-Pfa Saarland.

(Bild: plantic\Shutterstock.com)

Computervirus: Klinikum Fürth offline und mit eingeschränktem Betrieb

Im Netz des Krankenhauses treibt offenbar ein Trojaner sein Unwesen. Das Klinikum hat sich von der Notfallversorgung abgemeldet.

Das Klinikum Fürth ist nach einem PC-Virenbefall offline. (Bild: Billion Photos/Shutterstock.com)

Quelle: https://www.heise.de/security

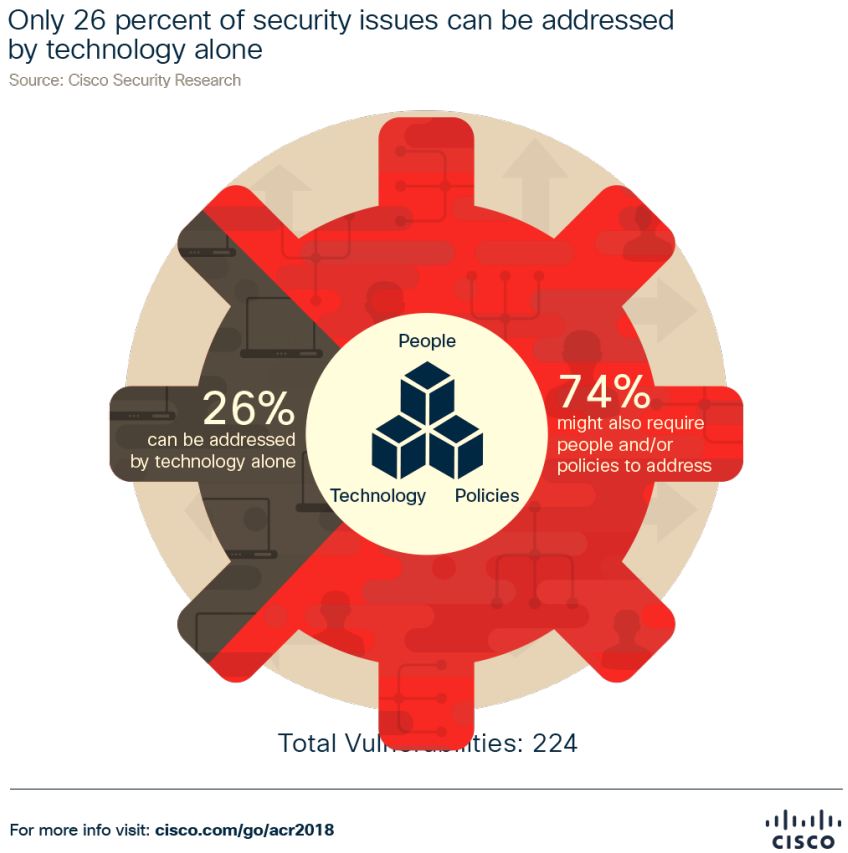
Cyber Security - Problem

Was ist das generelle Problem? Der Mensch!

- Cyber Security besteht aus Technik, Prozesse und Mensch
- Je mehr Sicherheitstechnik, desto mühsamer wird das Arbeiten
- Aus Effizienzgründen werden Sicherheitsaufgaben an den Menschen delegiert

Der Mensch ist bei allen Unternehmen ein integraler Teil des Schutzkonzept

Der Mensch lässt sich oft einfacher aushebeln als technische Lösungen

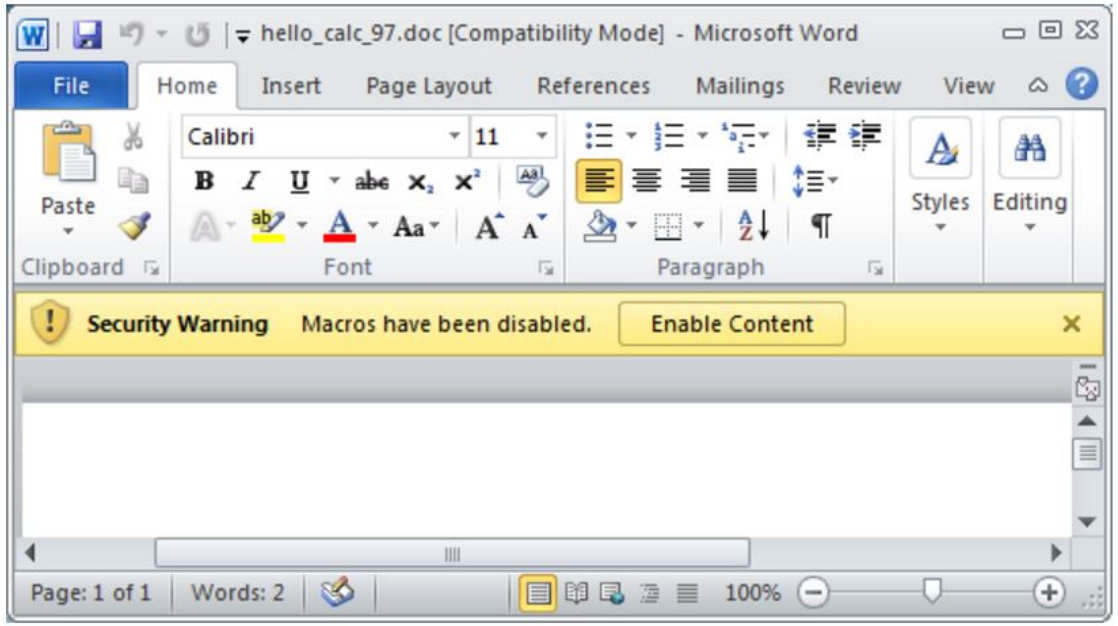


Cyber Security - Problem

Was ist das konkrete Problem? Das E-Mail!

Wussten Sie, dass eine Grosszahl der Angriffe

- … beim Mitarbeiter beginnen?
- … mittels E-Mails beginnen?
- … häufig Microsoft Office Makros verwendet?



Bin ich davon betroffen?

- die meisten Firmen sind schlecht gegen diese Angriffe geschützt
- auch gut geschützte Firmen werden Opfer
- der Klick eines einzelnen Mitarbeiters kann genügen

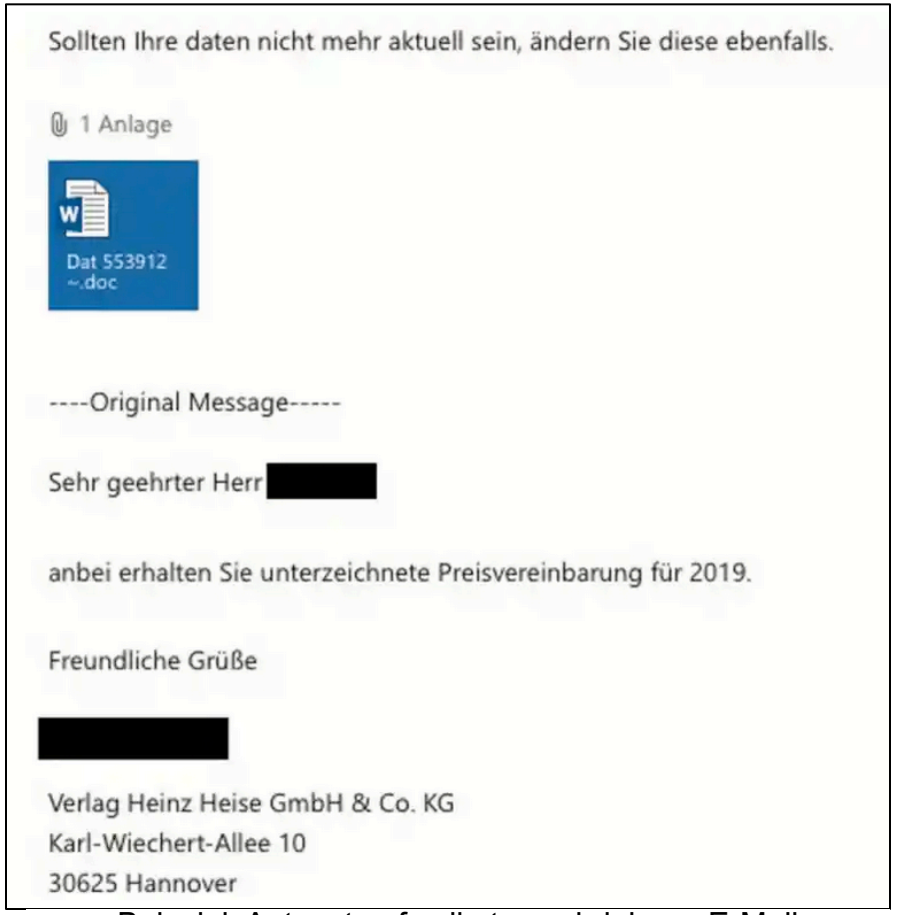
Cyber Security - Auswirkungen

Wieso ist dies ein Problem?

- Angriffstechnik wurden signifikant verbessert
- Redundante Schutzkonzepte werden auszuhebeln
- Mensch wird mit perfiden Tricks ausgehebelt

Ablauf heutiger Angriffe

- Kontextualisiertes Phishing E-Mail
- Interaktiver Hacker kommt auf infizierte System und attackiert Backup (Offline Backup vorhanden? Was heisst offline Backup?)
- Umsatzbasierte Lösegeldforderung (finanzieller Verlust)
- Publizierung der Daten bei Nicht-Bezahlen des Lösegelds (Imageschaden)


Sollten Ihre daten nicht mehr aktuell sein, ändern Sie diese ebenfalls.

1 Anlage

Dat 553912
~.doc

----Original Message-----

Sehr geehrter Herr [redacted]

anbei erhalten Sie unterzeichnete Preisvereinbarung für 2019.

Freundliche Grüße

[redacted]

Verlag Heinz Heise GmbH & Co. KG
Karl-Wiechert-Allee 10
30625 Hannover

Beispiel: Antwort auf selbst geschriebene E-Mail

Quelle: heise.de

Cyber Security - Massnahmen

Wie kann ich mich besser schützen?

1. Technische Sicherheit verbessern
2. Sicherheit verbessern, welche durch Mitarbeiter umgesetzt ist
    - Regelmässiges Training der Mitarbeiter
    - Regelmässiges Schulen der Mitarbeiter
    - Regelmässiges Testen der Mitarbeiter

Schwierigkeiten dabei

- Der Mensch vergisst schnell
- Verschiedene Angriffsmöglichkeiten (USB Stick, E-Mail, Telefon etc.)
- Cyber Security ist nicht plausibel und intuitiv
- Überprüfung der Lerninhalte schwierig
- Messen des Awareness-Levels schwierig
- Repression vs. Kooperation

Cyber Security - Massnahmen

Es braucht eine Strategie & ein Hilfsmittel

Aufgaben für den Security-Verantwortlichen

- Mitarbeiter müssen – zu ihrer eigenen Sicherheit - getestet werden
- Lerninhalte müssen zur Verfügung stehen
- Resultate müssen ausgewertet werden können
- Erhöhung der Sicherheit nur durch periodisches Training & Awareness
- Lernresistente Mitarbeiter müssen gezielt gefördert werden (Achtung Datenschutz)

Dieser Service ist komplex
und kann nur mit einem Tool effizient erbracht werden!

Fazit

Fakt:

Cyber Crime nimmt weiter zu

→Imageschäden und Kosten

Problem:

Angriffe zielen meistens auf die Mitarbeiter ab

Folge:

Es wird immer Training & Awareness brauchen

Als Prozess etablieren!

Notwendig:

Management Commitment, gute Strategie & gutes Werkzeug

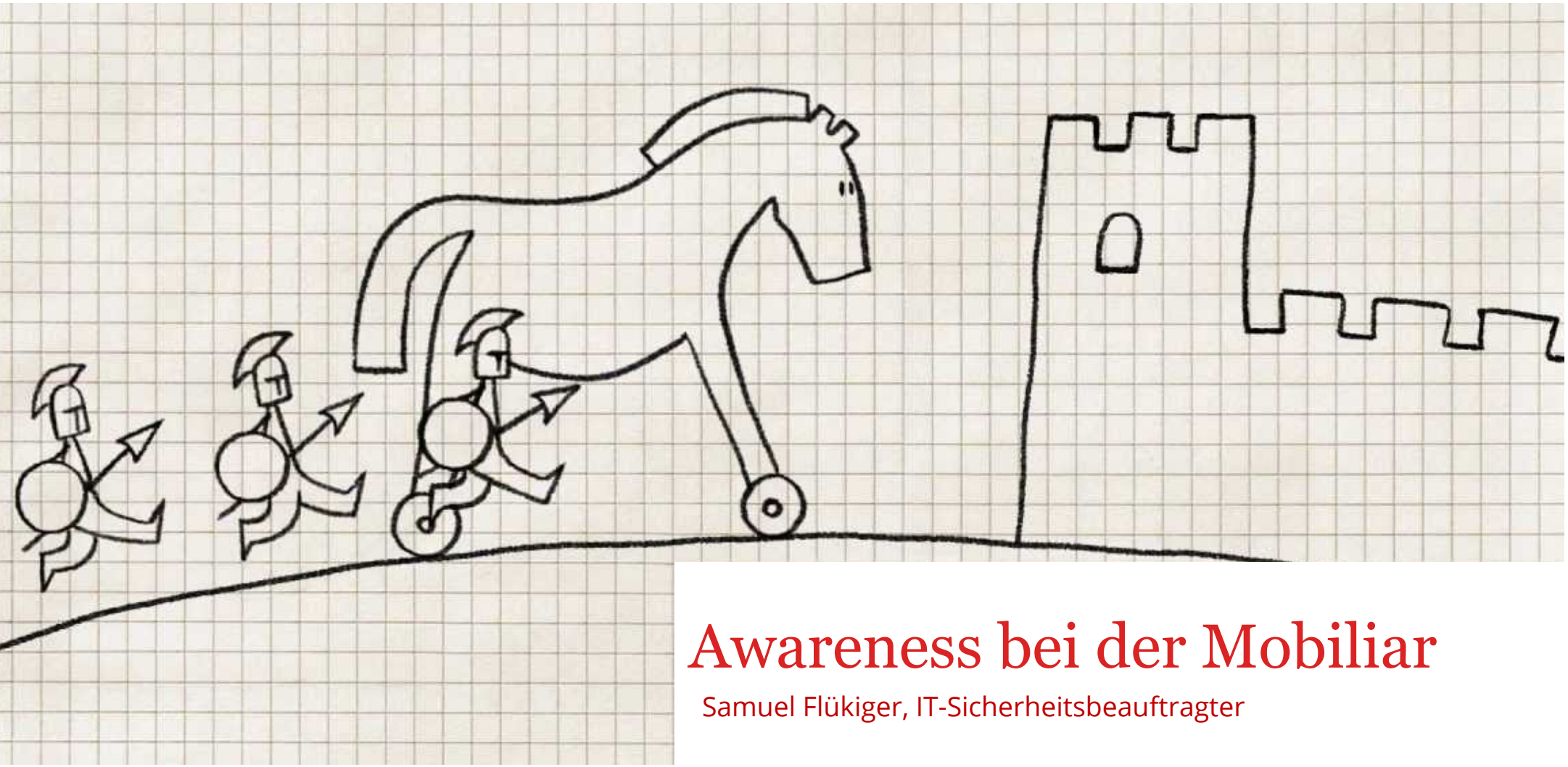
Handeln Sie, bevor auch Ihre Klinik still steht.

Ein starkes Team für Ihre Abwehr:

terreActive mit mehr als 20 Jahren Security-Erfahrung (Assessments, Audits, Pentests, Social Engineering etc.)

setzt auf Lucy für Pishing- & Awareness-Kampagnen

die Mobiliar



Awareness bei der Mobiliar

Samuel Flükiger, IT-Sicherheitsbeauftragter

Die Mobiliar auf einen Blick

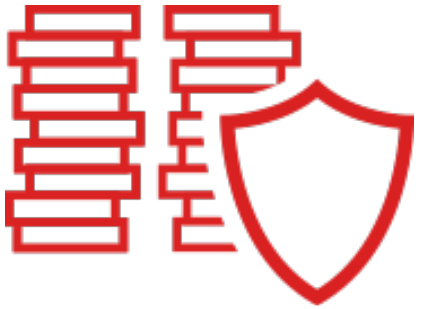
- Erste private Versicherungsgesellschaft der Schweiz
- Genossenschaftlich verankert
- 2 Mio. Kundinnen und Kunden
- Jährliches Prämienvolumen: CHF 3.8 Mia.
- Schweizer Marktführerin in Haushalt-, Betriebs- und Risikolebensversicherung
- 1/3 aller Haushalte und jedes 4. Unternehmen sind bei der Mobiliar versichert
- 9 von 10 Schadenfällen werden direkt vor Ort erledigt
- 79 Generalagenturen an 160 Standorten in der ganzen Schweiz
- Rund 5400 Mitarbeitende und über 300 Ausbildungsplätze

Cyber
Zwei Sichten für die Mobiliar

INTERN

Schutz der Geschäftsprozesse, Daten und IT-Systeme vor Cyber-Angriffen.

Die Mobiliar schützt ihre Geschäftsprozesse und Unternehmenswerte mit Cyber Security.



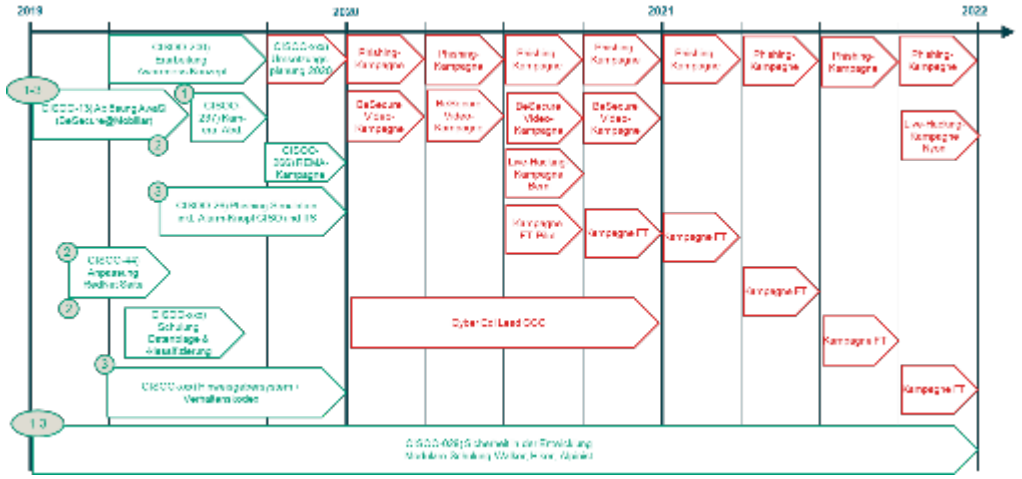
EXTERN

Kunden sichern Cyber-Risiken bei der Mobiliar ab.

Die Mobiliar hilft ihren Kunden die Cyber-Risiken zu bewältigen.

Mitarbeiter steht im Mittelpunkt
Sowohl bei Cyber-Angriffen als auch bei Sensibilisierung

- Mitarbeitende sind das einfachste und effizienteste Eintrittstor bei einem Cyber-Angriff.
- Mittels Phishing-Simulation können Mitarbeitende auf entsprechende Gefahren realitätsnah mit dem gewissen "Wau"-Effekt sensibilisiert werden.
- Jedoch darf eine Awareness-Konzept nicht alleine auf Phishing-Simulationen und Web-basierten Trainings beruhen.
- Eine Einbettung in ein Übergreifendes Konzept ist erforderlich.



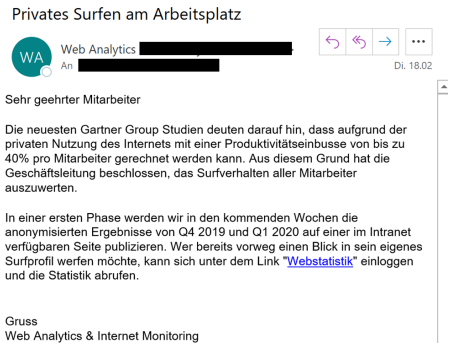
Phishing-Simulation bei der Mobiliar
Einsatz Lucy Security

Ziel

- Regelmässige Sensibilisierung der Mitarbeitenden (2 – 3 Phishing Kampagnen pro Jahr und Mitarbeitende)
- Mitarbeitende können einfach und schnell verdächtige E-Mails melden.

Umsetzung

- Seit November 2020 wird pro Monat für einen bestimmen Mitarbeiterkreis mindestens eine Kampagne durch-geführt.
- Mitarbeitende können verdächte E-Mails über einen Alarm-Knopf, welcher im E-Mail Client integriert ist melden.
- Meldungen werden direkt ans interne Cyber Defence Center (CDC) zur Analyse geschickt, teile der Analyse werden heute schon automatisiert (wird weiter ausgebaut).


Privates Surfen am Arbeitsplatz

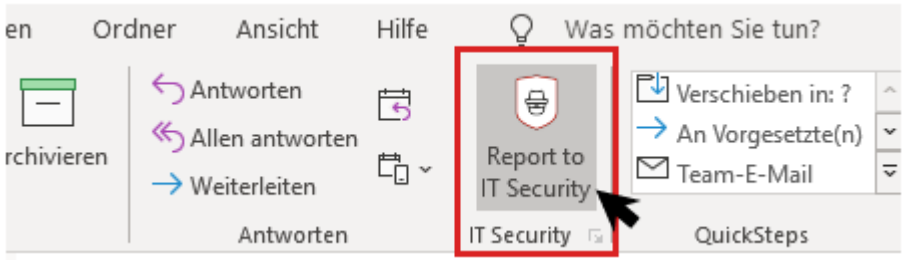
WA Web Analytics [redacted]
An [redacted] Di. 18.02

Sehr geehrter Mitarbeiter

Die neuesten Gartner Group Studien deuten darauf hin, dass aufgrund der privaten Nutzung des Internets mit einer Produktivitätseinbusse von bis zu 40% pro Mitarbeiter gerechnet werden kann. Aus diesem Grund hat die Geschäftsleitung beschlossen, das Surfverhalten aller Mitarbeiter auszuwerten.

In einer ersten Phase werden wir in den kommenden Wochen die anonymisierten Ergebnisse von Q4 2019 und Q1 2020 auf einer im Intranet verfügbaren Seite publizieren. Wer bereits vorweg einen Blick in sein eigenes Surfprofil werfen möchte, kann sich unter dem Link "Webstatistik" einloggen und die Statistik abrufen.

Gruss
Web Analytics & Internet Monitoring



Phishing-Simulation bei der Mobiliar Herausforderungen

Die Simulation soll keine Beübung der Sicherheits-organisation sein

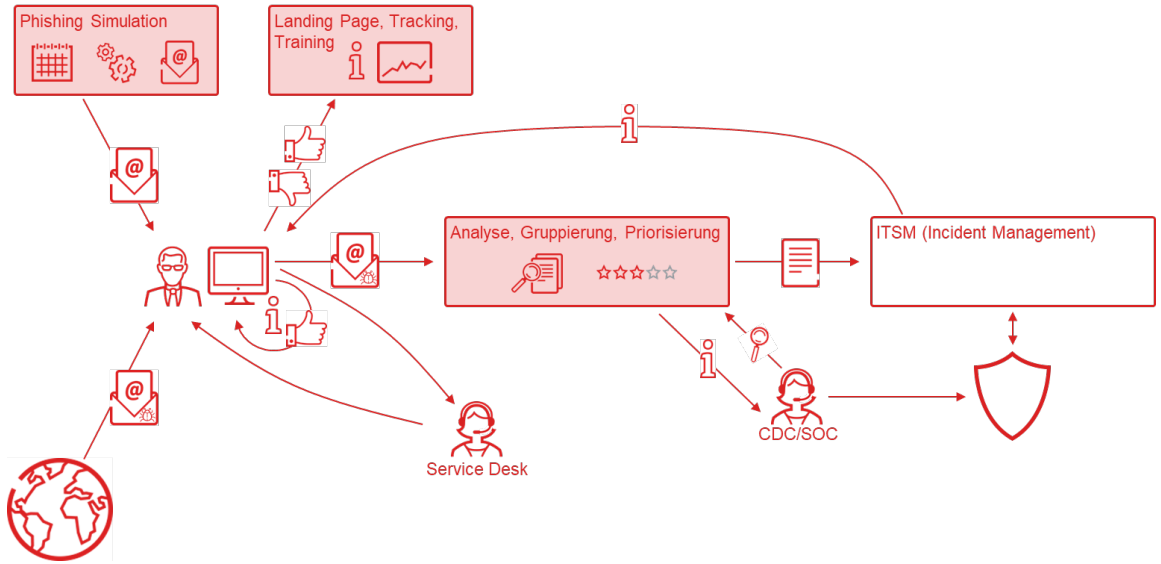
→ Ein Jahr von der Idee bis zur ersten Simulation

→ Wie integrieren wir Provider, Behörden, etc. in den Prozess?

Information aller relevanter Stakeholder vor Durchführung einer Kampagne

→ Wie kann verhindert werden, dass Service Desk und CDC durch entsprechende Simulationen überflutet werden?

Vereinfachung des Meldeprozess von verdächtigen E-Mails mittels Alarm-Knopf, automatische Triage von gemeldeten E-Mails, direkte und schnelle Rückmeldung an Mitarbeitende



Neue Funktion im Outlook: Alarm per Knopfdruck

Ab sofort können im Outlook mit Hilfe des Alarm-Knopfes «Report to IT Security» verdächtige E-Mails gemeldet werden. Weiter sind Sensibilisierungs-Kampagnen im Umgang mit Cyber-Risiken geplant.

Seit Neuestem ist im Outlook ein Alarm-Knopf (angeschrieben mit «Report to IT Security») integriert. Mit diesem Alarm-Knopf können Mobiliar Mitarbeitende verdächtige E-Mails direkt weiter melden. «Wir bieten den Alarm-Knopf im Mail-System an, damit verdächtige E-Mails sofort, einfach und unkompliziert gemeldet werden können», erklärt Philipp Locher, Leiter Cyber/IS/IT GRC & Reporting.

Einfacher und effizienter

Die verdächtige Nachricht wird direkt an unsere IT-Sicherheitsexperten vom Cyber Defence Center (CDC) weitergeleitet – ohne Umweg über den Service Desk IT. Das ist einfacher und effizienter, insbesondere bei akuten Phishing-Wellen, wenn statt der täglich rund 50 verdächtigen E-Mails auch mal 1000 und mehr an einem Tag gemeldet werden!

Grundsätzlich agieren Betrüger im Web immer raffinierter und gehen mitunter sehr professionell vor. Es wird immer schwieriger, gefälschte E-Mails von harmlosen zu unterscheiden. Bei der Mobiliar beispielsweise wurden im ersten Halbjahr 2019 über 1,1 Millionen E-Mails mit gefälschtem Absender abgefangen – das entspricht rund 15 Prozent aller E-Mails.

«Wenn nur ein einziger Mitarbeiter auf ein solches E-Mail hereinfällt, kann das grosse Konsequenzen für die Mobiliar nach sich ziehen», betont Philipp Locher. Hier trägt der Alarm-Knopf «Report to IT Security» merklich zu einer Vereinfachung für

"Alles in allem kann ich aber sagen, dass dies eine sehr gelungene Massnahme war und für reichlich Gespräche beim Kaffee gesorgt hat."

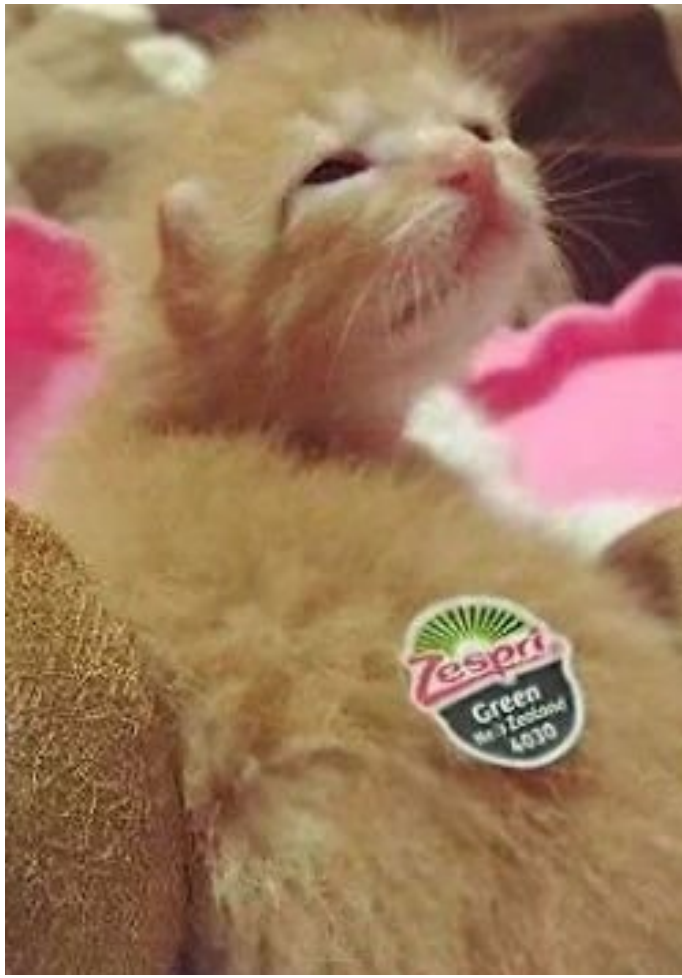
"Wenige Sekunden nachher am Helpdesk gemeldet und Password geändert aber ist schon zu spät. Nicht nett das nach 10 intensiven Stunden zu machen aber vollends korrekt – Hacker achten auch nicht darauf ob man am Tagesende kaputt ist und nicht mehr aufpasst. Mea culpa."

Ja, dieses Mal habt Ihr mich tatsächlich erwischt!
Zefix! Übel für mich, der ich sonst jedes eigenartige Mail mit Lucy melde…
Gut, dass Ihr solche Tests macht! DANKE.

Phishing-Simulation bei der Mobiliar
Erkenntnisse und Zahlen

- ~1200 Mitarbeiter bereits mit einer ersten Kampagne sensibilisiert.
- (Miss-)Erfolgsrate hängt stark
  - Komplexität der Kampagne
  - Zeitpunkt (7:30 vs. 10:00)
  - Grösse der Zielgruppe
  - Sensibilisierungsgrad
  - Wiederholungsfrequenz (max. 2 Monats-Effekt)

  ab.
- 0% ist nicht realistisch.
- Viel wichtiger ist jedoch die Melderate. Hier streben wir bis Ende 2020 >30% an.
- "Beübung" der Organisation hat durch eine durchgängige Planung und Integration in die Prozesse einen sehr geringen Impact auf den Betrieb.
- Meldung verdächtiger E-Mails durch Alarm-Knopf:
  - Reduktion Service Desk Anrufe um Faktor 10
  - Verdreifachung der Meldungen




Jeder braucht Security Awareness!
Und wir liefern es!
terreActive
terreActive
terreActive
terreActive
Lucy

Danke! Besuchen Sie uns am Stand, wir machen gerne eine Demo

terreActive AG
Kasinostr. 30, 5000 Aarau
+41 62 834 00 55
www.security.ch

LUCY Security AG
Chamerstrasse 44, CH-6300 Zug
Switzerland, +41 44 557 19 37
www.lucysecurity.com