



TAG DER OFFENEN TÜR, 12.09.2019

HERZLICH WILLKOMMEN!



BILDUNG. FREUDE INKLUSIVE.

SECURITY AWARENESS – CYBER CRIME

Workshop

Alexander Krenn, MSc.

Awareness Workshop

➤ Weil jeder Klick zählt



Hacker Wallpaper



Computer Hacker



Hacker Logo



Hacker Maske



Holzhacker



WER IST DER HACKER?



HTTPS://ABOUT:ALEXANDER

„Möchtegern Spitzensportler mit zu viel beruflichem Ehrgeiz.“



Rad-, Kletter- und Rudersportler

Allgemeine Informationssicherheit

- Was bedeutet Sicherheit?
- Das Internet
- Vorgehensweise eines Angreifers und wie sie sich schützen!

01

WIE IST SICHERHEIT ZU VERSTEHEN?

Maslowsche

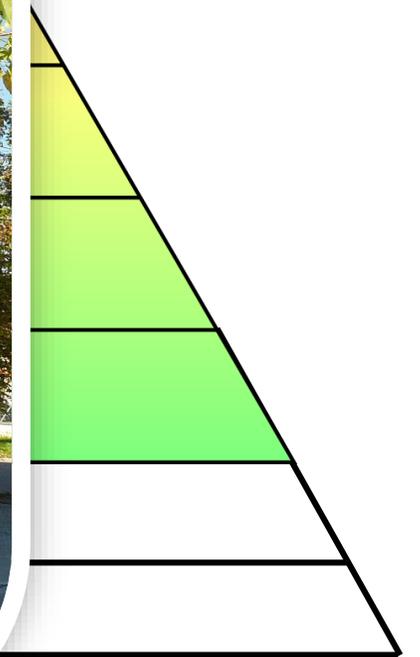
Ninas

Startups

Corporate

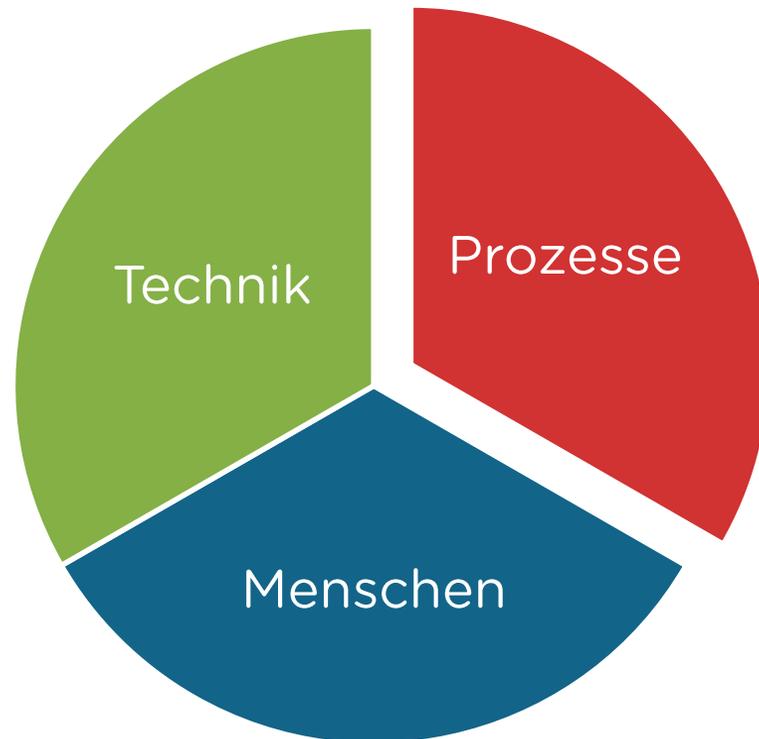


Die Raiffeisenbank Gammesfeld
(Computer seit April 2012)



3 SÄULEN

DER INFORMATIONSSICHERHEIT



Prozesse

Prozesse regeln den allgemeinen Umgang mit Informationen.

Technik

Firewalls, aktuelle Software, moderne Virens Scanner, E-Mail-Filter, aber auch Papier-Schredder, abschließbare Rollcontainer

Mensch

Computer schützen keine Informationen, wir Menschen machen das!

IM DETAIL: YOUTUBE

+20 Stunden Videocontent pro Sekunde

=1200 Stunden pro Minute

=72000 Stunden pro Stunde

=1728000 Stunden pro Tag

1728000 Stunden = **197 Jahre(!)**



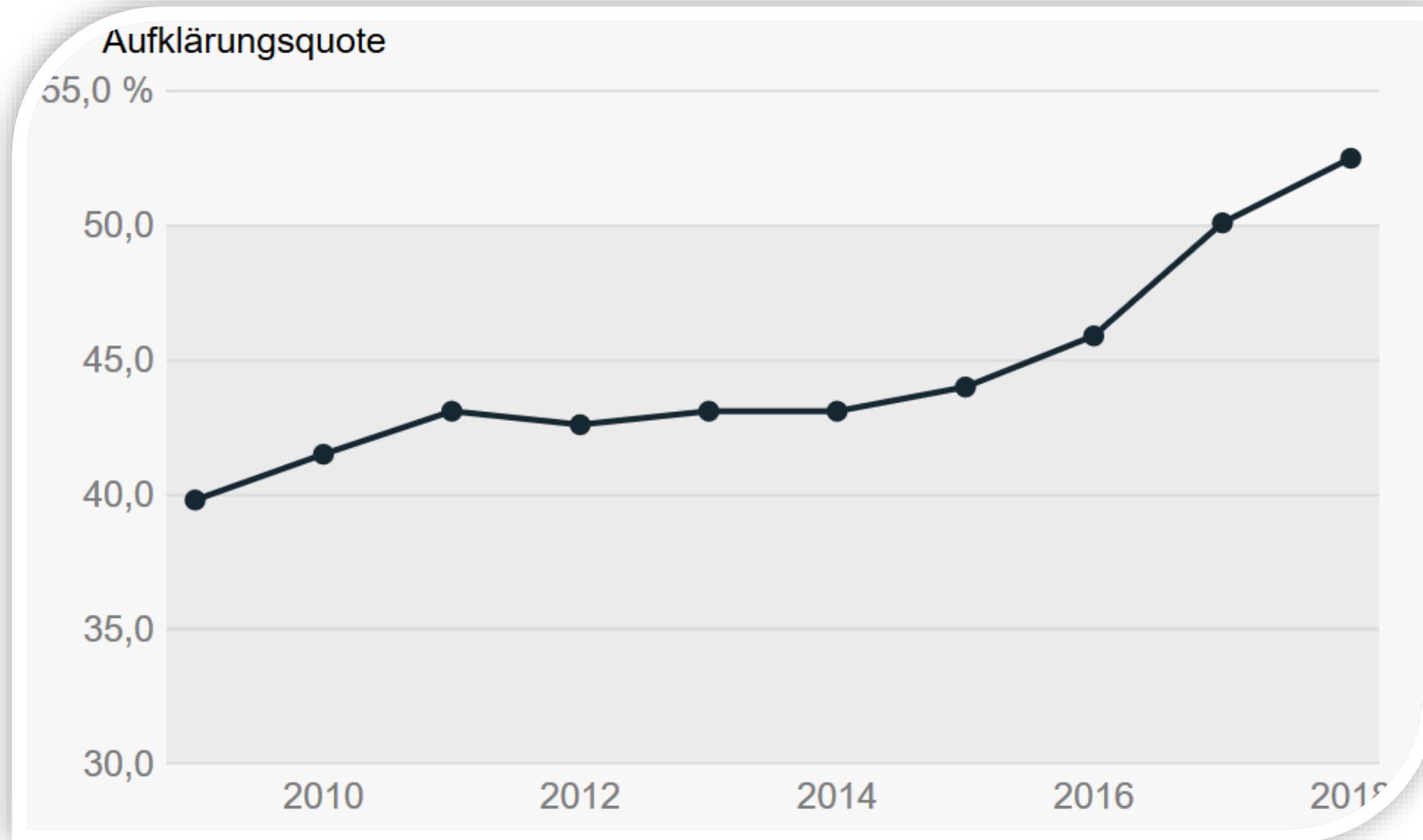
ENTWICKLUNG KRIMINALITÄT

Vergleich 1.HJ 2017 zu 1.HJ 2018 in Österreich

Bereich	2017	Veränderung 2017 zu 2018 in Prozent
Wohnungen und Wohnhäuser	-	-17,1%
Diebstahl von Fahrzeugen	-	-16,3
Gewaltdelikte	69.426	-4,3%

Quelle: <https://bundeskriminalamt.at/news.aspx?id=53457A393463735342686B3D>

ENTWICKLUNG AUFKLÄRUNGSRATE



**Aufklärungsrate 2018
Internetkriminalität:
37,4%**

EUGENE KASPERSKY IN ÖSTERREICH

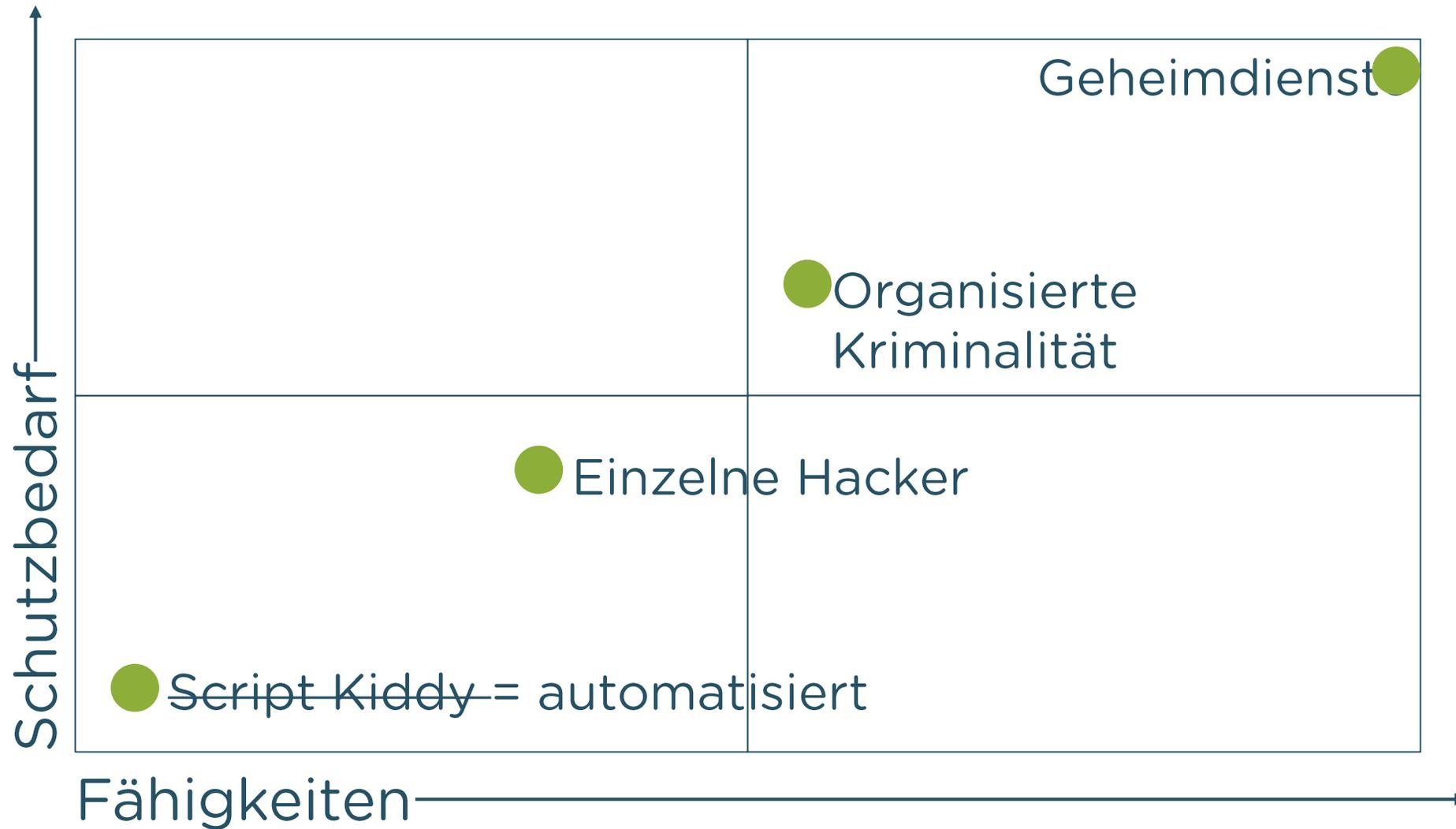
(2014) - ABER IMMER NOCH RELEVANT



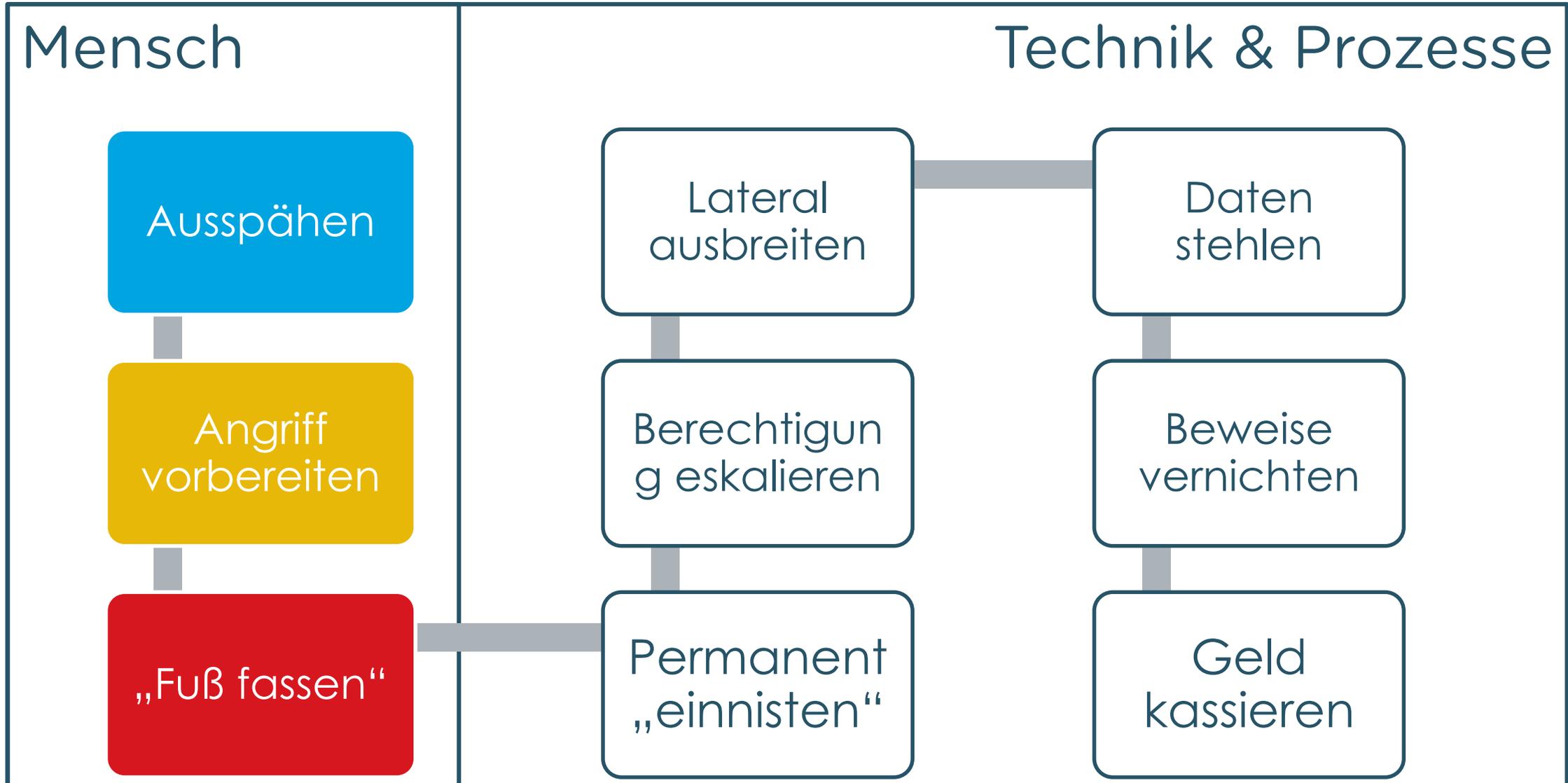
INTERNET+ÖSTERREICH=GRENZENLOS?



TYPEN VON ANGREIFERN



VORGEHENSWEISE DER ANGREIFER



WIE SIE SICH SCHÜTZEN

Physisch

- Kosten: Teuer, weil Aufwendig
- Erfolgsaussicht: Hoch
- Wiederholbarkeit: Gering - hinterlässt Spuren!

- ❖ Sperren sie ihren Bildschirm!
- ❖ Clean Desk
- ❖ Beobachtungen melden!
- ❖ Mobilgeräte beaufsichtigen!

Technisch

- Kosten: Gering, weil einfach
- Erfolgsaussicht: Durchschnitt
- Wiederholbarkeit: hoch - hinterlassene Spuren unbedenklich

- ❖ Seien sie achtsam bei E-Mails!
- ❖ Links prüfen, bevor sie klicken!
- ❖ Achtsamer Umgang mit Anhängen

Social

- Kosten: Gering, weil kaum Aufwand
- Erfolgsaussicht: Sehr hoch
- Wiederholbarkeit: hoch - hinterlässt kaum Spuren

- ❖ Geben Sie vertrauliche Informationen niemals über unvertrauenswürdige Kanäle weiter!
- ❖ Melden sie Verbesserungspotenziale!

SPIELANLEITUNG

➤ Fortress vs. Hackers™

MAX. 2 CHIPS JE SPIELRUNDE

SPIELRUNDE 1/3 (RECONNAISSANCE)



GEFÄHRDUNGSANZEIGER



SICHER

GEFÄHRDET

GEHACKT

GAME OVER

A-20 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

UNZUFRIEDENE KOLLEGE

Ein Kollege ist mit seiner Rolle im Unternehmen und seiner Bezahlung nicht zufrieden. Auch Mitarbeitergespräche können daran nichts ändern.

Aus Wut gibt er vertrauliche Informationen nach draußen. Die Konkurrenz verbietet es, ihn geschickt für eigene Zwecke zu nutzen.

Die Fortress AG legt das "Need-to-Know"- und 4-Augen-Prinzip und bemiht sich um ein gutes Arbeitsklima.

*Das Need-to-Know-Prinzip beschränkt, welche Daten von Mitarbeitern für die Erfüllung der Aufgaben verwendet werden dürfen und verhindert die Zugriffe anderer Mitarbeiter.

Risiko-Erfolgspunkte

4

A-18 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

UNTERNEHMENS BESICHTIGUNG

Regelmäßig besetzt die Fortress AG Unternehmensbesichtigungen an und zeigt dabei verschiedene Räumlichkeiten.

Ein besonders interaktiver Teilnehmer stellt einige Fragen zu laufenden Projekten, Mitarbeiterzahlen und Umsätzen.

Mitarbeiterinnen und Mitarbeiter, die Besichtigungen führen, werden besonders sensibilisiert, welche Informationen sie weitergeben dürfen.

Risiko-Erfolgspunkte

2

A-12 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

UNGESICHERTES W-LAN

Eine Mitarbeiterin verbindet sich auf dem Flughafen vor dem Abflug mit ihrem Smartphone über ein ungesichertes W-LAN*-Netz.

Unbekannte können nun Daten auslesen.

Durch Schulungen und Tests werden die Fortress AG, ihre Leute für die reflektierte Nutzung von W-LAN Vorbereitungen zu sensibilisieren.

*W-LAN oder Wi-Fi ist ein drahtloses Netzwerk, das Daten über ein drahtloses Netzwerk überträgt.

Risiko-Erfolgspunkte

3

A-10 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

SMARTPHONE VERBORGT

Ein Mitarbeiter kündigt der Fortress AG, bringt seinem Fahrrad-Kurierfahrer auf dem Heimweg sein Dienst-Telefon, damit er die Diebstahlsanzeige seines Fahradretter machen kann.

Das Smartphone ist nicht geschäftlich, weshalb problematische Daten eingeschoben und weitergesendet werden können.

Die Mitarbeiterinnen und Mitarbeiter werden instruiert, Dienst-Telefone zu sichern und prinzipiell nicht ohne Aufsicht anderen Personen zu überlassen.

Risiko-Erfolgspunkte

3

A-07 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

EINFACHE PASSWÖRTER

Ein Mitarbeiter der Fortress AG nutzt für dienstliche Konten einfach die selben Passwörter wie privat. Das Passwort ist nur 8 Zeichen lang und wenig komplex. Beispiel: "aaaaaaa".

Mit wenigen Versuchen kann sich der Angreifer in den WebMail-Account des Mitarbeiters einloggen.

Durch intensive und wiederholende Schulungen wird die Befolgung sicherer Passworter vermittelt.

Passwörter sollten formal und Passwörter erschützt sein.

Risiko-Erfolgspunkte

1

A-04 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

SOZIALE NETZWERKE

Ein Mitarbeiter der Personalabteilung twittert regelmäßig seine Gedanken und ist sehr aktiv auf Facebook. Auch seine beruflichen Gedanken sind eben stauffindend. Übernahme eines Mitarbeiter stellt er im Netz.

Konkurrenten recherchieren gezielt über soziale Netzwerke und Mitarbeiter, Firmeninterne vertraulich zu behandeln.

Die Fortress AG schult regelmäßig ihre Mitarbeiterinnen und Mitarbeiter, Firmeninterne vertraulich zu behandeln.

Risiko-Erfolgspunkte

4

FORRESS & ENTWICKLUNG

MAXIMUM 2 CHIPS

pro Runde dürfen hier investiert werden

→ In jeder Runde können Sie die Fortress AG durch den Einsatz von Chips unterstützen.

A-04 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

SOZIALE NETZWERKE

Ein Mitarbeiter der Personalabteilung twittert regelmäßig seine Gedanken und ist sehr aktiv auf Facebook. Auch seine beruflichen Gedanken sind eben stauffindend. Übernahme eines Mitarbeiter stellt er im Netz.

Konkurrenten recherchieren gezielt über soziale Netzwerke und Mitarbeiter, Firmeninterne vertraulich zu behandeln.

Die Fortress AG schult regelmäßig ihre Mitarbeiterinnen und Mitarbeiter, Firmeninterne vertraulich zu behandeln.

A-07 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

EINFACHE PASSWÖRTER

Ein Mitarbeiter der Fortress AG nutzt für dienstliche Konten einfach die selben Passwörter wie privat. Das Passwort ist nur 8 Zeichen lang und wenig komplex. Beispiel: "aaaaaaa".

Mit wenigen Versuchen kann sich der Angreifer in den WebMail-Account des Mitarbeiters einloggen.

Durch intensive und wiederholende Schulungen wird die Befolgung sicherer Passworter vermittelt.

Passwörter sollten formal und Passwörter erschützt sein.

A-10 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

SMARTPHONE VERBORGT

Ein Mitarbeiter kündigt der Fortress AG, bringt seinem Fahrrad-Kurierfahrer auf dem Heimweg sein Dienst-Telefon, damit er die Diebstahlsanzeige seines Fahradretter machen kann.

Das Smartphone ist nicht geschäftlich, weshalb problematische Daten eingeschoben und weitergesendet werden können.

Die Mitarbeiterinnen und Mitarbeiter werden instruiert, Dienst-Telefone zu sichern und prinzipiell nicht ohne Aufsicht anderen Personen zu überlassen.

A-12 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

UNGESICHERTES W-LAN

Eine Mitarbeiterin verbindet sich auf dem Flughafen vor dem Abflug mit ihrem Smartphone über ein ungesichertes W-LAN*-Netz.

Unbekannte können nun Daten auslesen.

Durch Schulungen und Tests werden die Fortress AG, ihre Leute für die reflektierte Nutzung von W-LAN Vorbereitungen zu sensibilisieren.

*W-LAN oder Wi-Fi ist ein drahtloses Netzwerk, das Daten über ein drahtloses Netzwerk überträgt.

A-18 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

UNTERNEHMENS BESICHTIGUNG

Regelmäßig besetzt die Fortress AG Unternehmensbesichtigungen an und zeigt dabei verschiedene Räumlichkeiten.

Ein besonders interaktiver Teilnehmer stellt einige Fragen zu laufenden Projekten, Mitarbeiterzahlen und Umsätzen.

Mitarbeiterinnen und Mitarbeiter, die Besichtigungen führen, werden besonders sensibilisiert, welche Informationen sie weitergeben dürfen.

A-20 RECONNAISSANCE

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

UNZUFRIEDENE KOLLEGE

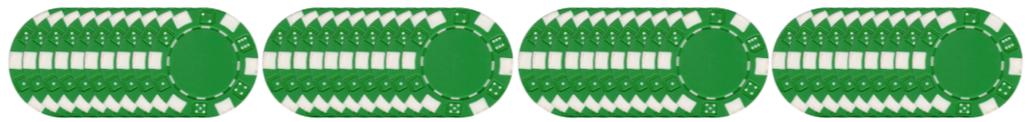
Ein Kollege ist mit seiner Rolle im Unternehmen und seiner Bezahlung nicht zufrieden. Auch Mitarbeitergespräche können daran nichts ändern.

Aus Wut gibt er vertrauliche Informationen nach draußen. Die Konkurrenz verbietet es, ihn geschickt für eigene Zwecke zu nutzen.

Die Fortress AG legt das "Need-to-Know"- und 4-Augen-Prinzip und bemiht sich um ein gutes Arbeitsklima.

*Das Need-to-Know-Prinzip beschränkt, welche Daten von Mitarbeitern für die Erfüllung der Aufgaben verwendet werden dürfen und verhindert die Zugriffe anderer Mitarbeiter.

RISIKO = EINTRITTSWAHRSCHEINLICHKEIT X AUSWIRKUNGEN



FORRESS US



HACKERS

Copyright © 2017 Alle Rechte vorbehalten. www.fortress-hackers.de

MAX. 2 CHIPS JE SPIELRUNDE

SPIELRUNDE 3/3 (GAINING ACCESS)



FORSCHUNG & ENTWICKLUNG

Maximal 2 Ressourcen-Chips pro Runde dürfen hier investiert werden

→ In jedem Angriffswellenfeld ist die Fortress AG den Gefährdungen angesetzt

FORTRESS US HACKERS®

GEFÄHRDUNGSANZEIGER

-7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

SICHER

GEFÄHRDET

GEHACKT

GAME OVER

C-01

LÜFTER

C-01

LÜFTER

C-01

LÜFTER

C-01

LÜFTER

C-01

LÜFTER

C-01

LÜFTER

C-01 GAINING ACCESS

LÜFTER

Der Lüfter des PCs ist seit einigen Tagen auffällig laut. Auch hat der Mitarbeiter das Gefühl, dass Anfragen plötzlich sehr lange dauern.

Der Angreifer hat eine Software installiert, die viel Rechenleistung beansprucht. Er hofft, dass der Mitarbeiter nichts bemerkt.

Die Fortress AG schützt ihre Mitarbeiter, auch auf plötzlich auftretende Auffälligkeiten bei technischen Geräten zu achten.

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

C-01 GAINING ACCESS

LÜFTER

Der Lüfter des PCs ist seit einigen Tagen auffällig laut. Auch hat der Mitarbeiter das Gefühl, dass Anfragen plötzlich sehr lange dauern.

Der Angreifer hat eine Software installiert, die viel Rechenleistung beansprucht. Er hofft, dass der Mitarbeiter nichts bemerkt.

Die Fortress AG schützt ihre Mitarbeiter, auch auf plötzlich auftretende Auffälligkeiten bei technischen Geräten zu achten.

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

C-01 GAINING ACCESS

LÜFTER

Der Lüfter des PCs ist seit einigen Tagen auffällig laut. Auch hat der Mitarbeiter das Gefühl, dass Anfragen plötzlich sehr lange dauern.

Der Angreifer hat eine Software installiert, die viel Rechenleistung beansprucht. Er hofft, dass der Mitarbeiter nichts bemerkt.

Die Fortress AG schützt ihre Mitarbeiter, auch auf plötzlich auftretende Auffälligkeiten bei technischen Geräten zu achten.

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

C-01 GAINING ACCESS

LÜFTER

Der Lüfter des PCs ist seit einigen Tagen auffällig laut. Auch hat der Mitarbeiter das Gefühl, dass Anfragen plötzlich sehr lange dauern.

Der Angreifer hat eine Software installiert, die viel Rechenleistung beansprucht. Er hofft, dass der Mitarbeiter nichts bemerkt.

Die Fortress AG schützt ihre Mitarbeiter, auch auf plötzlich auftretende Auffälligkeiten bei technischen Geräten zu achten.

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

C-01 GAINING ACCESS

LÜFTER

Der Lüfter des PCs ist seit einigen Tagen auffällig laut. Auch hat der Mitarbeiter das Gefühl, dass Anfragen plötzlich sehr lange dauern.

Der Angreifer hat eine Software installiert, die viel Rechenleistung beansprucht. Er hofft, dass der Mitarbeiter nichts bemerkt.

Die Fortress AG schützt ihre Mitarbeiter, auch auf plötzlich auftretende Auffälligkeiten bei technischen Geräten zu achten.

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

C-01 GAINING ACCESS

LÜFTER

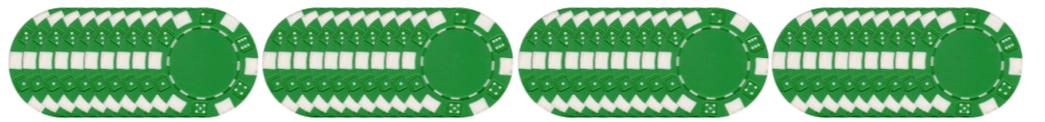
Der Lüfter des PCs ist seit einigen Tagen auffällig laut. Auch hat der Mitarbeiter das Gefühl, dass Anfragen plötzlich sehr lange dauern.

Der Angreifer hat eine Software installiert, die viel Rechenleistung beansprucht. Er hofft, dass der Mitarbeiter nichts bemerkt.

Die Fortress AG schützt ihre Mitarbeiter, auch auf plötzlich auftretende Auffälligkeiten bei technischen Geräten zu achten.

Risiko = Eintrittswahrscheinlichkeit x Auswirkung

RISIKO = EINTRITTSWAHRSCHEINLICHKEIT X AUSWIRKUNGEN



Persönliche Datenschutzrichtlinie erstellen

➤ Formulare austeilen

Key – Takeaways Give-Aways

- Was von dem heute Gelernten macht Sinn?
- Was werde ich umsetzen/verändern?
- Kann ich das Gelernte weitertragen/teilen?
- Was können wir in der Firma noch machen? Ideen!
- Weitere Training in Geschäftsbereichen sinnvoll?

FIN



TAG DER OFFENEN TÜR, 12.09.2019

DANKE FÜR IHR INTERESSE!



BILDUNG. FREUDE INKLUSIVE.

Möchten Sie die Unterlagen von [diesem und allen anderen Vorträgen/Workshops](#) vom heutigen Tag der offenen Tür in [digitaler Form](#) zugeschickt bekommen, dann füllen Sie bitte folgendes Online-Formular aus:

www.bfi.wien/workshops