Bundesverband Medizinische Versorgungszentren-Gesundheitszentren-Integrierte Versorgung e.V.

BMVZ

DigiTrace

Dipl.-Wirt.-Inf. Martin Wundram

Datenschutz & Datensicherheit bei aktuellen ePA-Projekten

Warum IT-Sicherheit echte Arbeit ist und Nicht-Sicherheit keine Option

15. März 2019

Wintertreffen - Arbeitstreffen der BMVZ-Mitglieder 14. & 15. März 2019, Hamm

Kurzvorstellung

PERSON

- **Martin Wundram**
- Jahrgang 1982
- Diplom Wirtschafts-informatik, Uni Köln

wundram@digitrace.de

ERFAHRUNG (AUSWAHL)

Von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung, **insbesondere IT-Sicherheit und IT-Forensik**

Lehrbeauftragter der Universität zu Köln

Geschäftsführer DigiTrace GmbH (Standort Köln: 7 Personen)

Kunden von KMU bis DAX + Behörden

- Präventive Projekte: Audits, Penetrationstests, IT-Sicherheitskonzepte, strategische Beratung zu IT-Sicherheit, …
- Reaktive Projekte: IT-Forensik, Incident Response, eDiscovery, …
- Sachverständigentätigkeit / Gutachten zu allen Themen der IT

Gründungs- und Vorstandsmitglied im Bundesverband für den Schutz Kritischer Infrastrukturen e.V. (bski.de)

Agenda

BMVZ

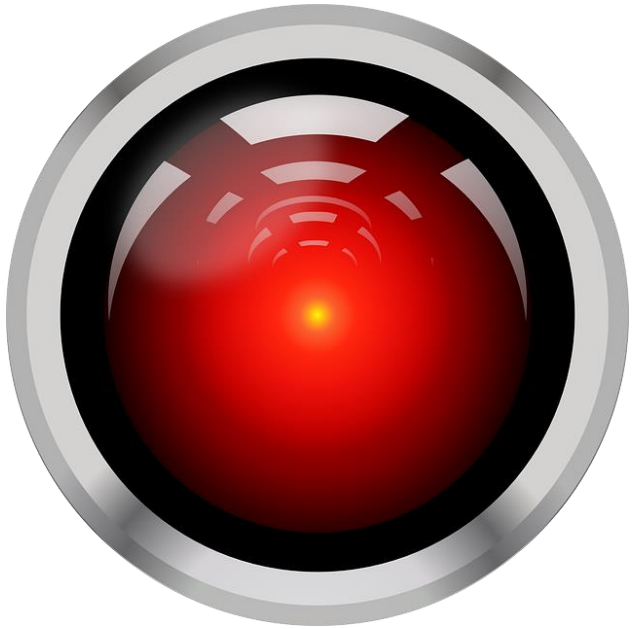
Warum IT-Sicherheit echte Arbeit ist und Nicht-Sicherheit keine Option

(60 Minuten inkl. Fragen und Diskussion)

1	Die Bedrohung ist real
2	Live Hacking
3	Handlungsempfehlungen
4	Fazit und Ausblick

Die Bedrohung ist real

- Bitte überlegen Sie kurz: wie ist Ihre Einschätzung zu folgenden Fragen:
  - Haben wir noch die volle Kontrolle über unsere Daten? Ja/Nein? Warum?
  - Haben Sie etwas (Daten?) zu verbergen? Ja/Nein? Warum?
  - Was ist Sicherheit?



Die Bedrohung ist real - Sicher?

DigiTrace

Die Bedrohung ist real - Sicher?

DigiTrace

Die Bedrohung ist real – Scheinbar sicher!

DigiTrace

Das mehrfach unsichere Vorhängeschloss

- Es gibt einzelne Techniken (Schloss, Bügel, Tür, …) die für sich genommen sicher oder unsicher sein können (gemessen am Schutzbedarf)
- Diese müssen jedoch implementiert werden (Auswahl, Planung, Montage, Test).
- Bei jeder dieser Phase kann etwas schief gehen, so dass im Ergebnis trotz sicherer Technik ein unsicheres Gesamtsystem entsteht

- Erkannte Probleme:
  - Beschlag lässt sich abschrauben
    - falsche Auswahl
  - Schloss lässt sich horizontal drehen, so kann der Riegel ohne Schlossöffnung so weit geöffnet werden, dass er nicht mehr sperrt
    - Fehlplanung und/oder Fehlmontage
  - Gesamtsystem ist damit nicht wirksam gegen die (mutmaßlich zu verhindernden) Bedrohungen
    - nicht ausreichend getestet

Die Bedrohung ist real

Murphys Gesetz: und was wir daraus für die Informationssicherheit lernen können

- **„Alles, was schiefgehen kann, wird auch schiefgehen.“,**
  John W. Campbell Jr.
  - „Zweijähriger fällt in mehr als hundert Meter tiefes Bohrloch - In Spanien ist ein Kleinkind in ein nur 25 Zentimeter breites, 110 Meter tiefes Bohrloch gefallen. In dem Erdloch ist es feucht und kalt, die Retter kämpfen gegen die Zeit.“, Quelle: spiegel.de
  - Nichts einfach so auf die leichte Schulter nehmen, nicht den Kopf in den Sand stecken, aber auch keine Angst haben
  - Risikomanagement ist die Grundmaxime

Die Bedrohung ist real

DigiTrace

Leitgedanke

- Sicherheit erfordert von Anfang an und konstant Arbeit und Einsatz
- Sicherheit kann man nicht einfach „einkaufen“
- Das schwächste Glied der Kette bricht
- Noch wichtiger als Modelle, Rahmenwerke, Theorie und Schlagworte ist, angstfrei die Thematik ernst zu nehmen und in den eigenen Alltag angemessen zu integrieren

Die Bedrohung ist real

DigiTrace

Wesentliche Erkenntnisse

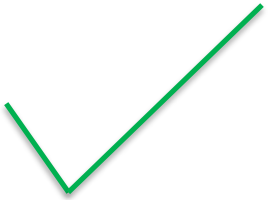
- Nichts ist sicher, question everything
- Sicherheit kostet Geld / Komfort / Freiheit / …
- „Unsere“ Daten haben mittlerweile aus vielen Gründen hohen Wert für Andere
- Das schwächste Glied der Kette bricht. Ein System muss insgesamt sicher sein. Manchmal reicht „ein falsches Bit“, und das ganze System ist unsicher
- Problembewusstsein ist die erste und vielleicht sogar wichtigste Maßnahme der Informationssicherheit
- Sicherheit des Entwurfs / Architektur / „Bauplans“ vs. Sicherheit des konkreten Produktes
- Safety vs. Security

Die Bedrohung ist real

Was sollen wir tun? Strategische „Marschrichtung“?

~~Angst~~

„Die gesunde Mitte finden“



~~Weiter machen, wie bisher~~

„Es gibt nichts Gutes, außer man tut es“

Die Bedrohung ist real

DigiTrace

Aus der Rolle eines Arztes

Die Bedrohung ist real

DigiTrace

Aus der Rolle eines alltäglichen PC-Benutzers

Die Bedrohung ist real

DigiTrace

Anti-Viren-Programme: Ein Allheilmittel?

- Tavis Ormandy von Google hat *mehrere* Lücken in *mehreren* Anti-Viren-Produkten gefunden!
- Ausführung beliebigen Schadcodes auf Anwender-PCs
- Auslesen von gespeicherten Passwörtern (Passwortmanager) aus der Ferne
- Der „Secure-Browser“ verwendet veralteten Quellcode und ist

  „das Lächerlichste, was ich je gesehen habe“

Auch fehlende wirksame Sicherheitsprodukte sind ein (unlösbares?) Problem

Die Bedrohung ist real

Wert der Daten

- Nicht neu: **Wissen ist Macht**

- Neu: Der **Wert von Daten** hat in den letzten Jahren enorm zugenommen

- Großen Anteil hat der Netzwerkeffekt
  - Stichwort Suchmaschinenanbieter, der gleichzeitig ein soziales Netzwerk, E-Mail, Instant Messaging, Collaboration und Co. anbietet

- Aber auch: **Neue Qualität von Daten**

Siehe exemplarisch: http://www.trendmicro.de/infografiken/wie-viel-sind-ihre-daten-wert/

Die Bedrohung ist real

DigiTrace

Die Gefahr von Cyber-Schäden in Zahlen

Studie PwC, 2015:

- Jedes **zehnte** Unternehmen wurde 2014 mindestens einmal Opfer eines Angriffes über das Internet
- Durchschnittlicher **wirtschaftlicher Schaden:** 80.000 Euro
- Durchschnittlicher Schaden ein Jahr zuvor: 10.000 EUR

Umfrage IHK Berlin-Brandenburg, 2017:

- Jedes **vierte** Unternehmen von Hackerangriffen betroffen
- 50% der Einbruchsdiebstähle werden angezeigt, nur 10 % der Hackerangriffe

- 500 bis 750 Mrd. Euro Schäden durch Computerkriminalität weltweit
  (Cyber-Kriminalität – das unterschätzte Risiko, GDV, 10.03.2014)
- Zusätzlich: Schäden durch allgemeine Ausfälle (z.B. Festplattendefekte)

Quelle: http://www.heise.de/newsticker/meldung/Studie-Mittelstand-unterschaetzt-Gefahr-durch-Cyber-Kriminalitaet-3067640.html
https://www.ihk-berlin.de/blob/bihk24/3780186/bd8693d5e97aca59baeb77ede6bce94a/Kriminalitaetsbarometer_2017-data.pdf

Die Bedrohung ist real

Beispiele

Computersicherheit: 18-Jähriger findet 190.000 ungeschützte Festplatten im Netz

Von Christian Stöcker

Ein Student kann sich ganz in Ruhe auf Festplatten rund um die Welt umsehen - weil sie völlig ungeschützt am Netz hängen. Auf den Rechnern findet er Erstaunliches: Passwörter, illegale Filmkopien, geheime Dokumente.

Quelle: SpiegelOnline

Die Bedrohung ist real

Beispiele: Abfluss vertraulicher Daten – Mitarbeiter wechseln mit Daten

Finanzieller Schaden: unbezifferbar, oft >25.000 EUR

Die Bedrohung ist real

DigiTrace

Es trifft Kleine wie Große

- **Sony-Hack, Ende 2014**
  - Tätergruppe wollte Veröffentlichung des Films „The Interview“ verhindern
  - Angebliche Angriffsdauer: 1 Jahr, angeblich 100 TB Daten abgegriffen
  - Rückstellung für Q1 2015: 15 Mio. USD

- **Ashley Madison-Hack, Mitte 2015**
  - Tätergruppe hat über 25 GB interne Daten einer Dating-Plattform erbeutet und veröffentlicht (inkl. ca. 40 Mio. Kundendatensätze)
  - Erpressungsversuch der Täter blieb erfolglos – Ashley Madison ging an die Öffentlichkeit
  - Folgen: unter anderem mindestens ein Suizid

Die Bedrohung ist real

DigiTrace

Es trifft Kleine wie Große

- **Panama Papers, Mossack-Fonseca 2016**
  - Anonymer Whistleblower hat 2,5 TB interne Geschäftsdaten des Unternehmens geleakt
  - Rund 11,5 Mio. Briefe, Verträge, Urkunden, Rechnungen, …
  - zahlreiche Ermittlungsverfahren folgten

- **2017: Equifax, Cellebrite, Shadowbrokers**

- **2018: Aadhaar** (indische ID-Datenbank)**, Marriott, MyHeritage, Cathay Pacific, …**

Die Bedrohung ist real

Status quo?

25.01.2019 12:51 Uhr | Security

Neue Passwort-Leaks: Insgesamt 2,2 Milliarden Accounts betroffen

Nach der Passwort-Sammlung Collection #1 kursieren nun auch die riesigen Collections #2-5 im Netz. So überprüfen Sie, ob Ihre Accounts betroffen sind.

Von **Ronald Eikenberg**

04.01.2019 09:02 Uhr

Hackerangriff: Persönliche Dokumente von deutschen Politikern und Promis veröffentlicht

Unbekannte haben angebliche persönliche Daten und parteiinterne Dokumente deutscher Politiker und anderer Prominenter veröffentlicht.

Von **Oliver Bünte**

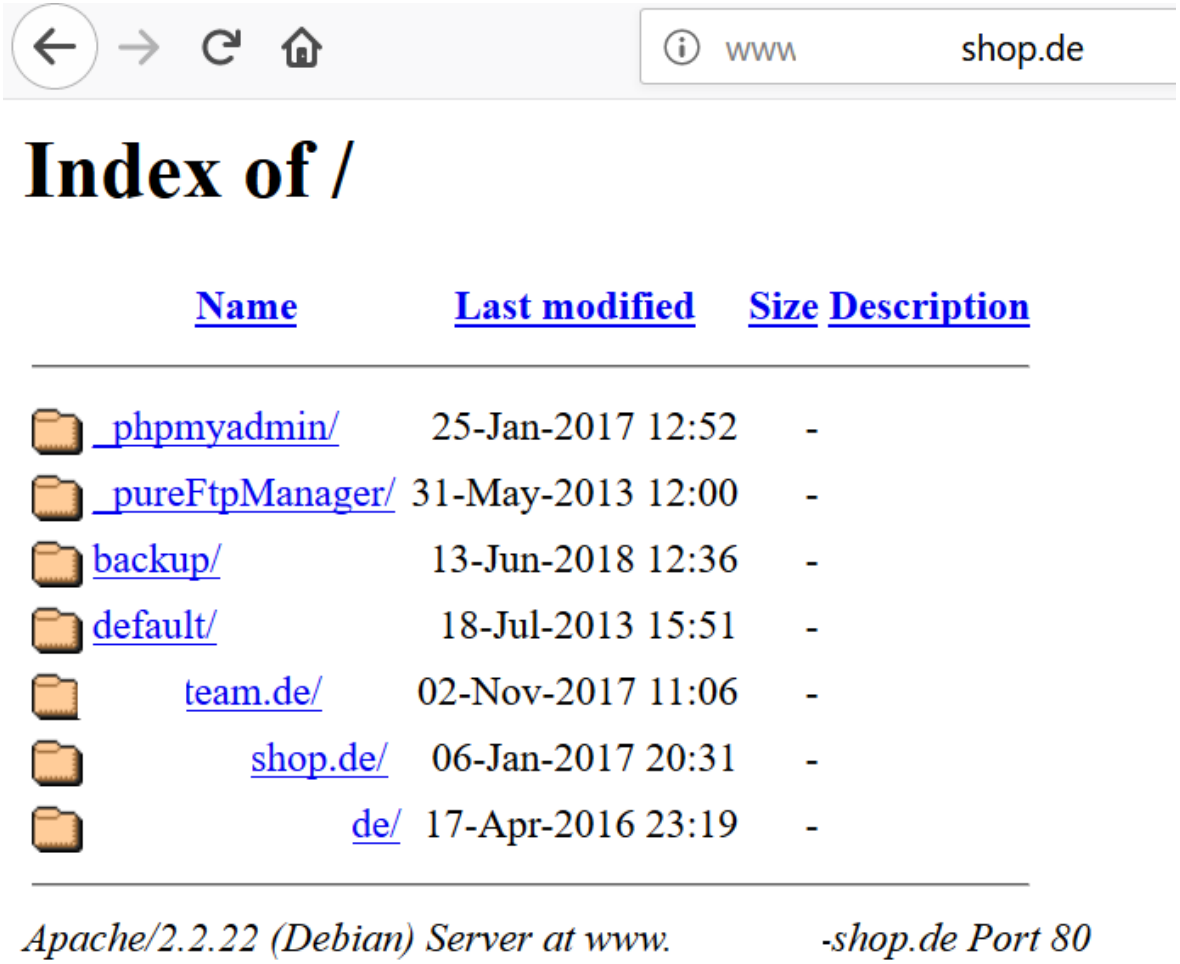
965

Quelle: alle Heise Online

Die Bedrohung ist real

DigiTrace

Incident Response ist für Viele immer noch völlig neu und ungeübt



Die Bedrohung ist real

DigiTrace

In drei einfachen Schritten zur Katastrophe

1. Alltäglicher Defekt an einem wichtigen Server inkl. Datenverlust
2. Das Backup wurde falsch konfiguriert – es wurde täglich nur ein leerer Ordner gesichert…
3. Aufgrund eines bestehenden Versicherungsschutzes wurde eine extrem teure Datenrettung beauftragt (x00.000 EUR)

Ergebnis:

- Versicherung möchte nicht zahlen (verständlich)
- Dienstleister wird in Regress genommen (x00.000 EUR, verständlich)
- Dienstleister ist insolvent

Die Bedrohung ist real

DigiTrace

Tätergruppen / Tätermöglichkeiten und Tätermotivation

- Akteure lassen sich klassifizieren nach
  - **Fähigkeit**: Sicherheitsexperten, Exploit-Programmierer, „Script-Kiddies“
  - **„Farbe“:** White-, Grey-, Black-Hat
  - **Motivation:** Spaß, Ansehen, wirtschaftliche, politische oder militärische Interessen
  - **Organisation:** Einzeltäter, lokale Gruppe, (weltweite) vernetzte Gruppe
  - **Beziehung zum Opfer:** Innentäter, Außentäter
- Täter rangieren dabei vom
  - **„Spaßtäter“** über
  - **„einfache“ Kriminelle** und organisierte Kreise bis hin zu
  - **staatlich geförderten** oder aufgestellten Täterkreise: Spionage, Cyber-War
- zielgerichtete vs. „Massenangriffe“
- **Möglichkeiten der Täter nehmen mit der immer stärkeren Vernetzung unserer Welt weiter zu**

Die Bedrohung ist real

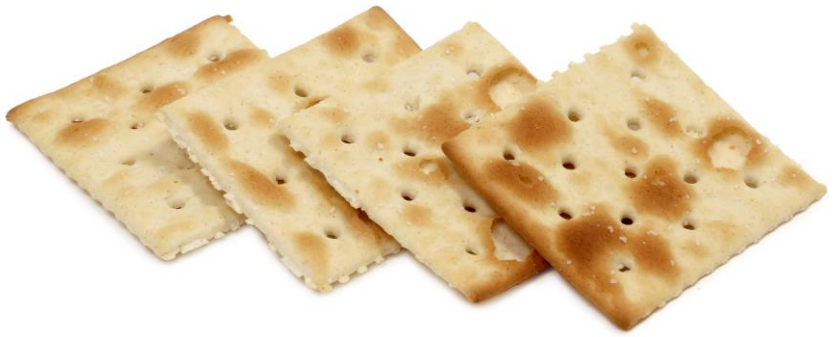
Tätergruppen / Tätermöglichkeiten und Tätermotivation

Hacker spähten Online-Banking Login-Daten aus. xijian/iStock.com

Dienstag, 03.01.2017, 15:37

Professionelle Hacker knacken fast alles, wie vor kurzem der Angriff

Quelle: focus.de



Hacker

Cracker

Die Bedrohung ist real

DigiTrace

Tätergruppen / Tätermöglichkeiten und Tätermotivation

„Ein Hacker ist jemand, der versucht einen Weg zu finden, wie man mit einer Kaffeemaschine Toast zubereiten kann.“

-- Wau Holland, Mitgründer des Chaos Computer Clubs

„ **Cracker** (vom englischen *crack* für „knacken“ oder „[ein]brechen“) umgehen oder brechen Zugriffsbarrieren von Computersystemen und Rechnernetzen.“

-- Wikipedia, Cracker (Computersicherheit)

Hacker

Cracker

Live Hacking

DigiTrace

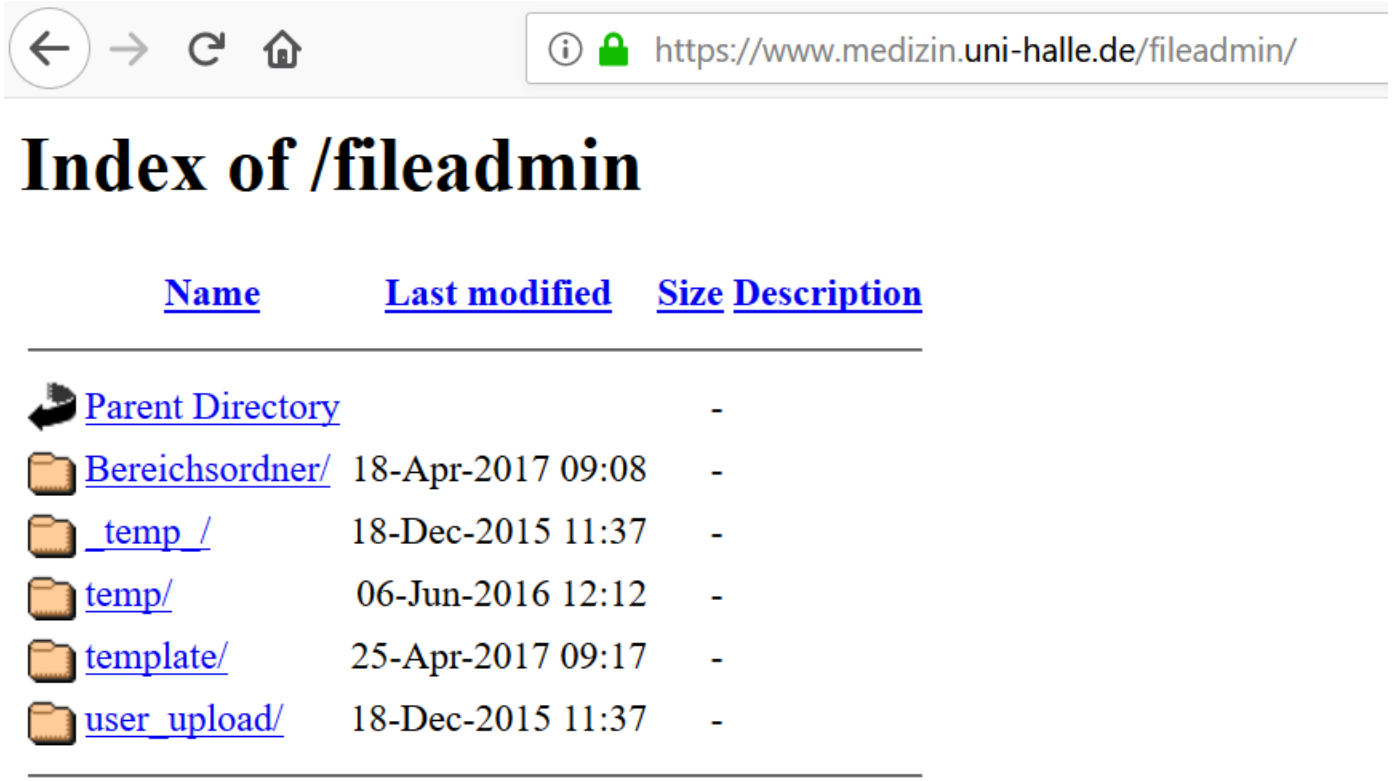
Hacking von der heimischen Couch mit Google

- „Erfunden“ z.B. von Johnny Long (USA)
- Google indexiert Webseiten und folgt dabei Links auf Ressourcen, nutzt aber auch weitere Techniken, um möglichst viel Web-Inhalte zu finden
- Es gibt etliche spezielle Suchtechniken, die insbesondere auch zum Hacken verwendet werden können, etwa
  - index of inurl medizin

Live Hacking

DigiTrace

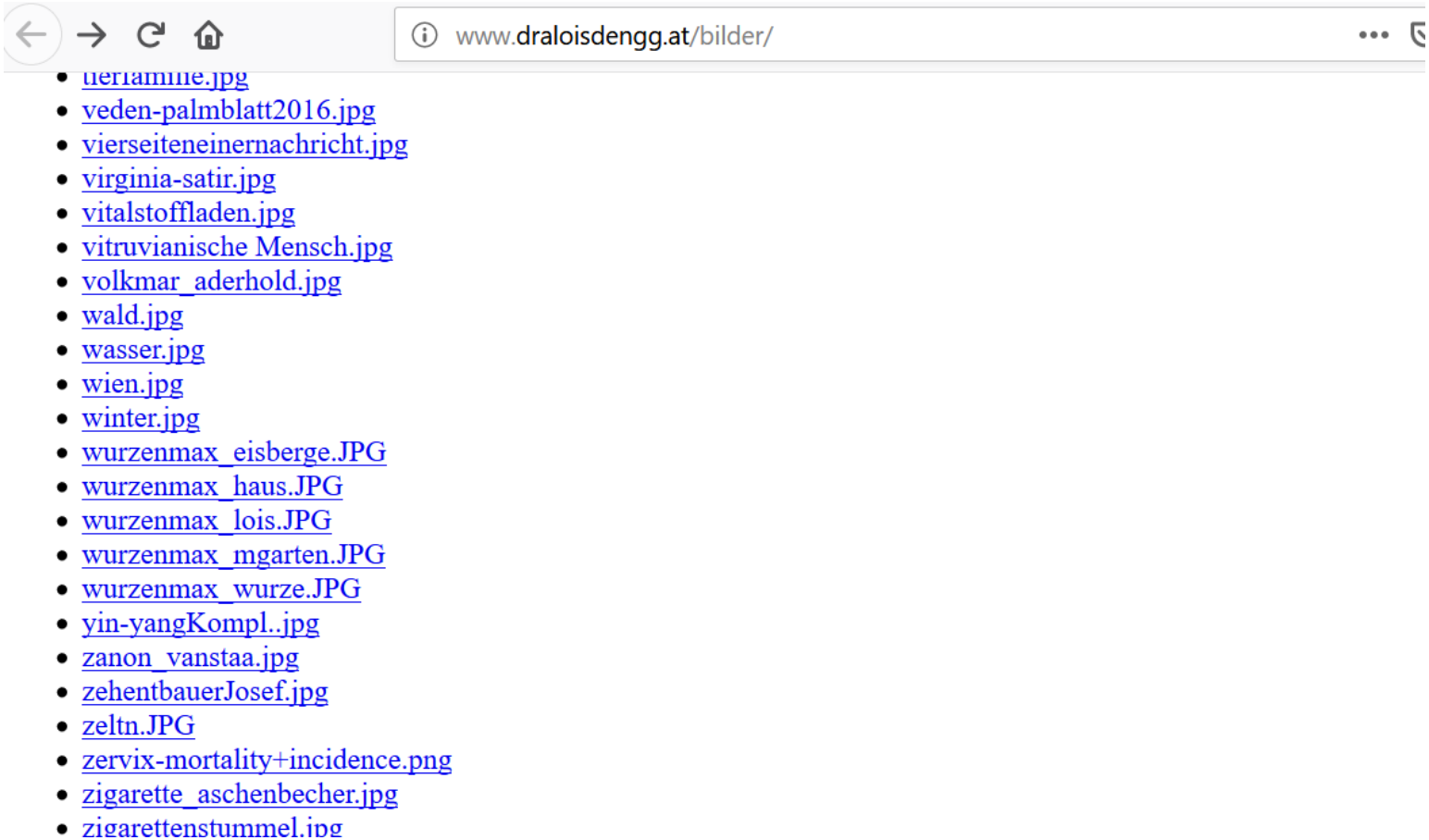
Hacking von der heimischen Couch mit Google



Live Hacking

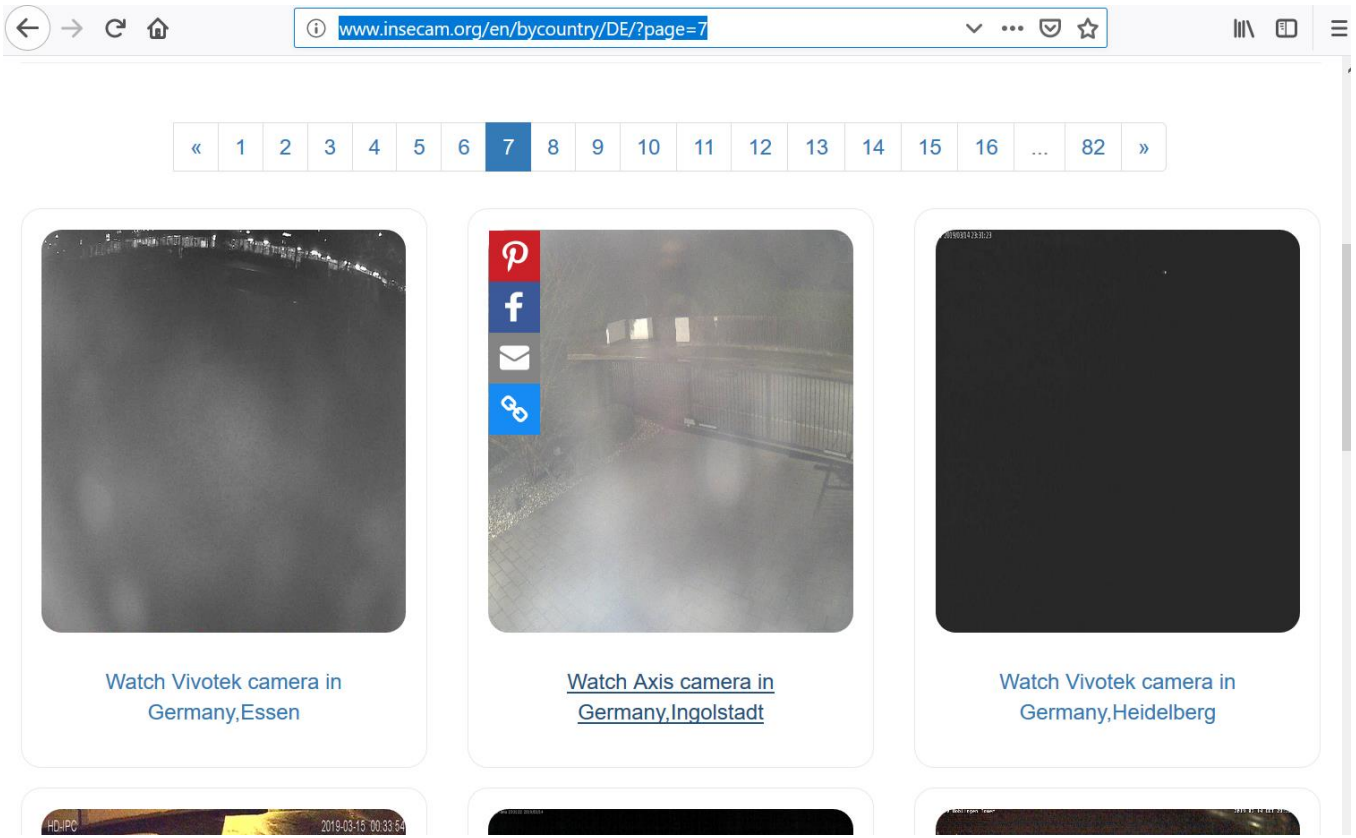
DigiTrace

Hacking von der heimischen Couch mit Google



DigiTrace

Katastrophen finden wie am Fließband für Jedermann mit Insecam.org



Handlungsempfehlungen

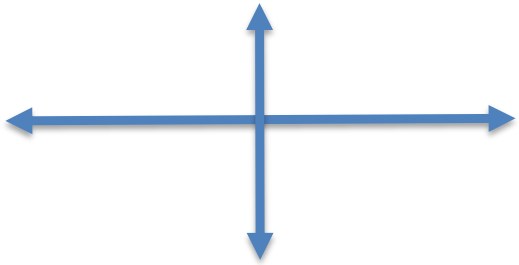
- Interagierende Systeme können in der Praxis nicht 100% sicher sein, aber „20% reicht nicht“
- Mit der Annäherung an 100% steigt der Aufwand überproportional
- Komfort vs. Sicherheit
- Einem großen Teil der Angriffsvektoren kann man jedoch bereits mit einfachen Maßnahmen begegnen

Handlungsempfehlungen

Selbst Kompetenzen aufbauen

Juristische Herausforderungen

Strategische / taktische Herausforderungen



Finanzielle Herausforderungen

Technische Herausforderungen

Verantworten muss letztlich der Geschäftsführer/Inhaber/Arzt

Handlungsempfehlungen

DigiTrace

Netzwerk- und Systemtrennung

- **Schlecht**:
  - Aus dem WLAN auch Systeme im LAN erreichen können
  - Nur ein WLAN, auch für Gäste
  - Ein PC für alle Aufgaben (Office, Web, E-Mail, …)
  - Ein Mobiltelefon für alle Aufgaben
  - Vernetzte Standorte, mit der Möglichkeit von überall jedes andere IT-System erreichen zu können
  - Vertrauliche Daten in unsicheren (Shared)-Cloud-Umgebungen
- **Gut**:
  - Gäste-WLAN, WLAN wie ein externes Netzwerk betrachten (VPN)
  - Durch Firewalls getrennte Teilbereiche: IT-Administration, Entwicklung, Produktion, Standort A, Standort B, …
  - 1 PC für Web und E-Mail + 1 PC für vertrauliche Dokumentbearbeitung

Handlungsempfehlungen

DigiTrace

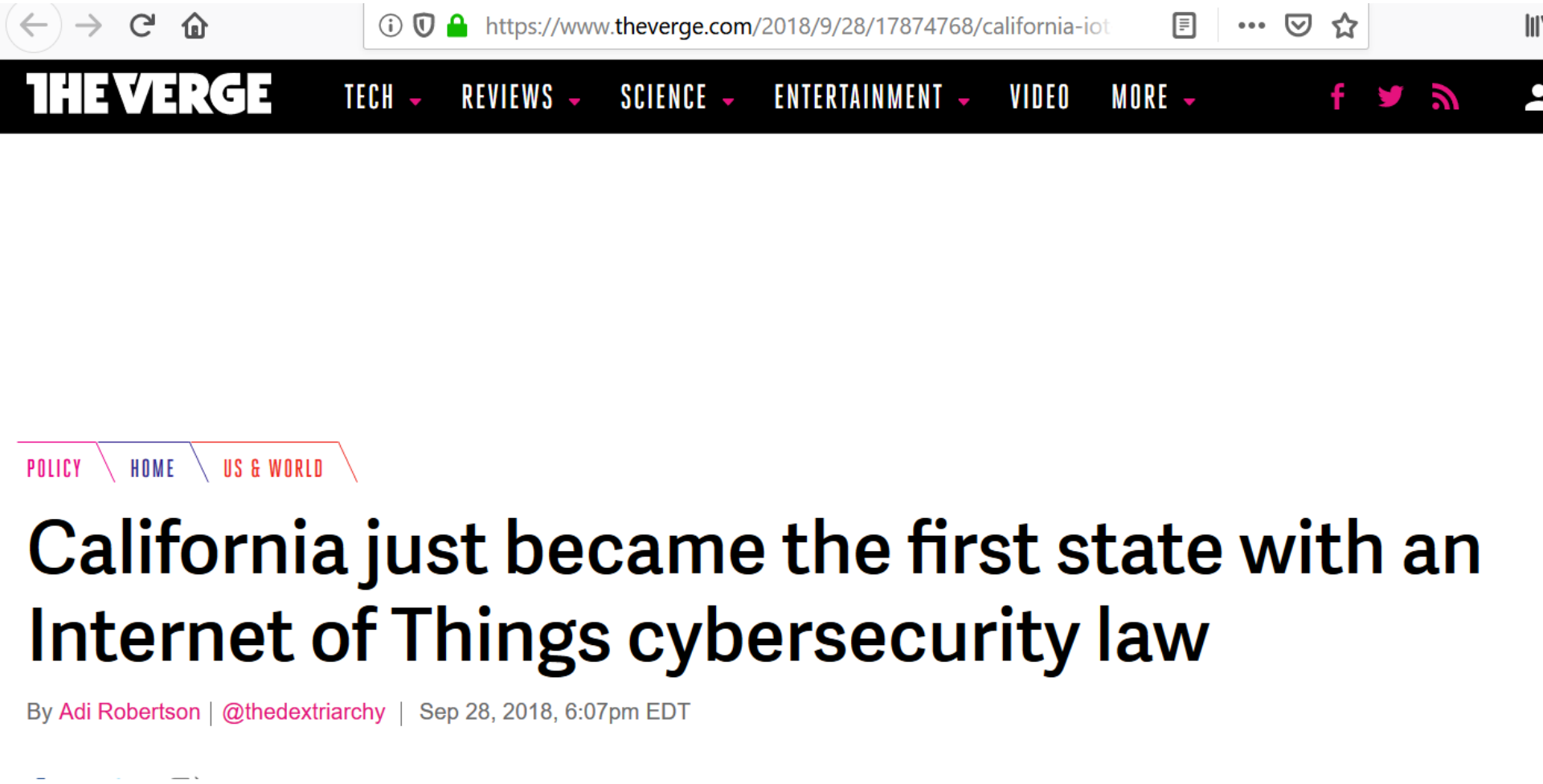
Fordern Sie sichere Systeme ein

- IT-Unsicherheit eher als Mangel werten, als bisher
- Penetrationstests und sichere Prozesse von Anbietern/Kunden verlangen (Kosten klären)
- Aktiv Anforderungen an Anbieter/Kunden setzen
- Rückfragen stellen, Zustand bestätigen lassen und evtl. sogar selbst überprüfen (Audit)

Handlungsempfehlungen

DigiTrace

Gestalten Sie rechtzeitig eine geeignete Regulierung



Handlungsempfehlungen

Penetrationstests

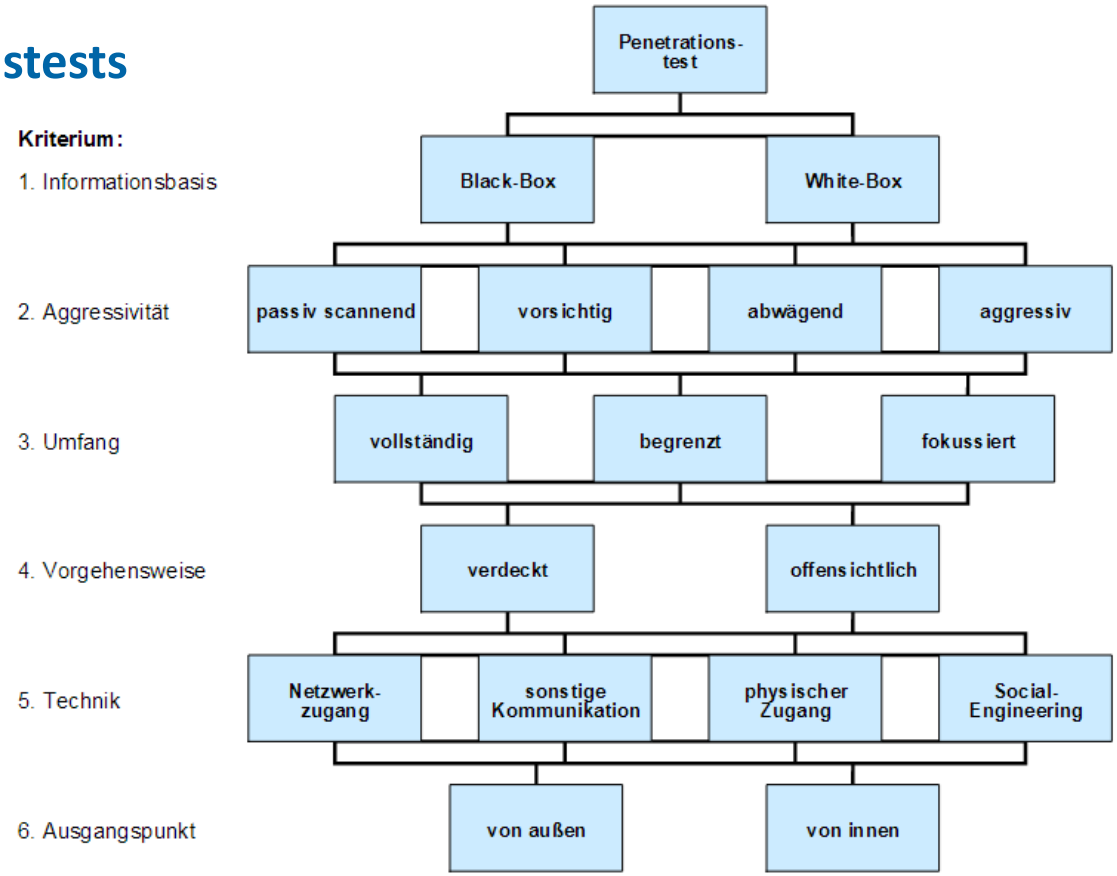


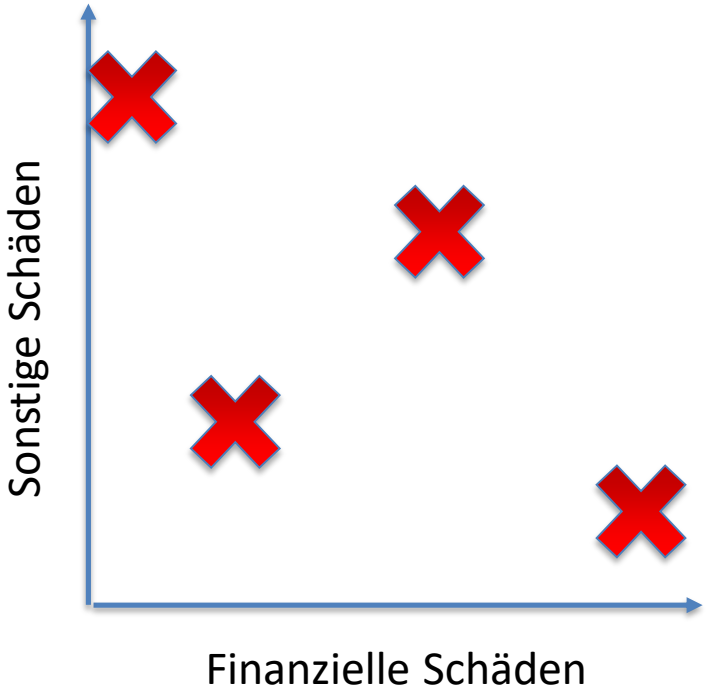
Abbildung 1: Klassifikation von Penetrationstests

- Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest_pdf.pdf?__blob=publicationFile

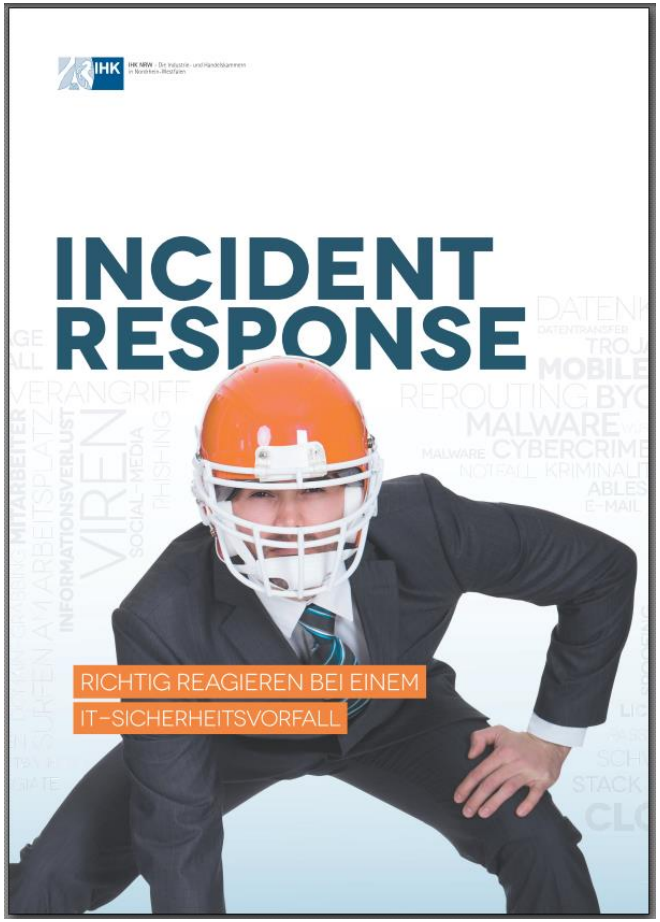
Handlungsempfehlungen

DigiTrace

Versicherbarkeit: Finanzielle vs. sonstige Schäden



Leitfaden Incident Response



DEFINITION

IT-SICHERHEITSVORFALL (INCIDENT)

Ereignis analog einem Notfall, das die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen, für welche Sie einen hohen oder sehr hohen Schutzbedarf definiert haben, in Ihrem Unternehmen / Ihrer Organisation derart beeinträchtigt, dass ein großer Schaden für Ihr Unternehmen / Ihre Organisation / Ihre Kunden oder Geschäftspartner entstehen kann.

RICHTIG REAGIEREN BEI EINEM IT-SICHERHEITSVORFALL

Bewahren Sie Ruhe und lassen Sie den Ernst der Lage prüfen. Egal ob ein „unachtsamer Klick' oder ein fortgeschrittener IT-Angriff - nur mit Ihrer rechtzeitigen Unterstützung und Mitarbeit können interne oder externe Experten den Fall aufklären und lösen.

Die nachfolgende Liste soll Ihnen helfen, bei einem möglichen IT-Sicherheitsvorfall bestmöglich zu handeln. Wir empfehlen Ihnen daher, diese Liste sofort greifbar aufzubewahren.

1. Reagieren Sie überlegt aber zügig. Erzeugen Sie möglichst keine Aufregung im Unternehmen. Weder auf die lange Bank schieben noch Panik sind gute Lösungen.
2. Prüfen Sie welche Personen vertrauenswürdig oder voreingenommen sind bzw. möglicherweise im Fokus stehen. Holen Sie dann Expertenrat ein. Qualifizierte Fachexperten sollten rechtzeitig eingebunden werden. Bilden Sie gegebenenfalls ein Krisenreaktionsteam. Sorgen Sie für eine verlässliche Unterstützung durch Ihren externen Dienstleister.
3. Priorisieren Sie Ihr weiteres Vorgehen und weihen Sie nur erforderliche und vertrauenswürdige Personen ein.
4. Stellen Sie wenn möglich betroffene Geräte, Daten und Backups sicher. Prüfen Sie, ob alle wichtigen Daten in einem funktionsfähigen Backup vorhanden sind. Achten Sie auf die Vollständigkeit, Aktualität und Integrität der Daten. Lassen sich gesicherte Daten wirklich öffnen und zurückspielen?
5. Wenn das Smartphone oder ein anderes Mobilgerät abhandengekommen ist, prüfen Sie, ob verbundene Dienste oder Accounts abrufbar sind und sperren Sie diese bei Bedarf.
6. Verändern Sie die Daten nicht, um keine Spuren zu verwischen. Arbeiten Sie stattdessen mit geeigneten (forensischen) Kopien.
7. Dokumentieren Sie den Vorfall sorgfältig. Protokollieren Sie dazu durchgeführte Schritte und Ihre Beobachtungen umfangreich und genau, z.B. durch Fotos und exakte Zeitangaben.

   Beispiel: Am 01.04. um ca. 14:30 Uhr habe ich eine E-Mail mit einem angehängten Lieferschein erhalten. Die ZIP-Datei habe ich geöffnet, aber nicht gespeichert. Es öffnete sich kurz ein schwarzes Fenster. Ansonsten ist nichts passiert. Am darauf folgenden Tag konnte ich keine Word-Dateien mehr öffnen. Auf meinem Bildschirm erschien eine Warnung des FBI bezüglich illegaler Aktivitäten mit einer Zahlungsaufforderung zwecks Strafe. Anbei befindet sich ein Foto von der Warnung, das ich mit meinem Handy erstellt habe.
8. Entwickeln Sie unterschiedliche Szenarien:
   - Wie reagiert man auf einen Innentäter?
   - Wie reagiert man darauf, wenn Kundendaten in fremde Hände geraten sind?
   - Wie lassen sich verlorene Daten wiederherstellen?
   - Was ist, wenn die eigenen IT-Systeme nicht mehr vertrauenswürdig sind?

„Better safe than sorry – Ein Fehlalarm ist besser als ein übersehener Sicherheitsvorfall."

EINFACHE PRÄVENTIVE MASSNAHMEN

Am besten sind Sie gut vorbereitet! Dazu hilft ein aktueller und vollständiger Infrastrukturplan (Was steht wo, Netzwerkplan, Konfiguration), ein Incident Response Plan (Liste zum „Abarbeiten' für den Ernstfall) und die präventive Kontaktaufnahme mit Ihren IT-Dienstleistern. Erarbeiten Sie mit diesen gemeinsam einen (kleinen) Plan, der die wichtigsten Punkte und Maßnahmen kurz skizziert.

https://www.ihk-koeln.de/upload/IHK_Leitfaden_Incident_Response_DINA4_05_54030.pdf

Handlungsempfehlungen

Goldene Tipps für den Ernstfall

- ☑ Prüfen Sie, wer vertrauenswürdig ist
- ☑ Priorisieren Sie das weitere Vorgehen
- ☑ Arbeiten Sie forensisch „sauber“
- ☑ **Gehen Sie von Anfang an koordiniert vor**
- ☑ **Dokumentieren Sie den Vorfall genau**
- ☑ Binden Sie relevante Personen ein
- ☑ Stellen Sie ein Krisenteam zusammen
- ☑ Entwickeln Sie verschiedene Szenarien

Fazit

Anwenderseite:

- Sicherheit erwarten, im Zweifel einfordern
- Kritisch hinterfragen
- Thematik Ernst nehmen

- „zum Glück“: die Masse der Angriffe erfolgt ungerichtet

Informationssicherheit betrifft jeden und steigt „in der Agenda“ zunehmend weiter nach oben

Ausblick

- Zunahme von IT-Sicherheitsvorfällen und deren Schadenausmaß extrem wahrscheinlich

- Unternehmen/Organisationen müssen sich vorbereiten
- Professionelle Unterstützung (durch Ihre IT-Experten) wird immer wichtiger

- **Auch und besonders als IT-Anwender muss man sich „leider“ mit Aspekten der Informationssicherheit beschäftigen**

- Denn: die Welt der IT und des Internet befinden sich in einer Phase der noch immer zunehmenden Risiken

Diskussionsrunde / Ihre Fragen

- Sind Ihre Systeme und Ihre Daten ausreichend sicher?
- Wie könnten Sie Ihre Informationssicherheit erhöhen?
- Inwieweit sind Sie bereit, für Sicherheit auf Komfort zu verzichten?
- Was bedeutet das für den Umgang mit Informationen allgemein?
- Was bedeutet das für (ihr) Unternehmen?
- Müssen wir jetzt Angst haben?
- …

Gerne auch im Nachgang an
wundram@digitrace.de