

User Awareness

Das Beste IDS der Welt

Götz Weinmann (Bereichsleitung TOsecurity Strategie)



Verizon Data Breach Report 2018

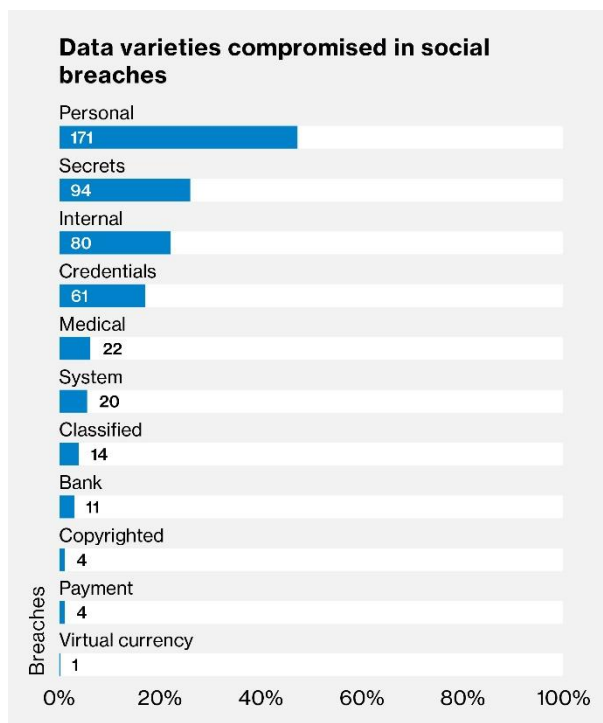


Figure 12. Data varieties compromised in Social breaches (n=362)

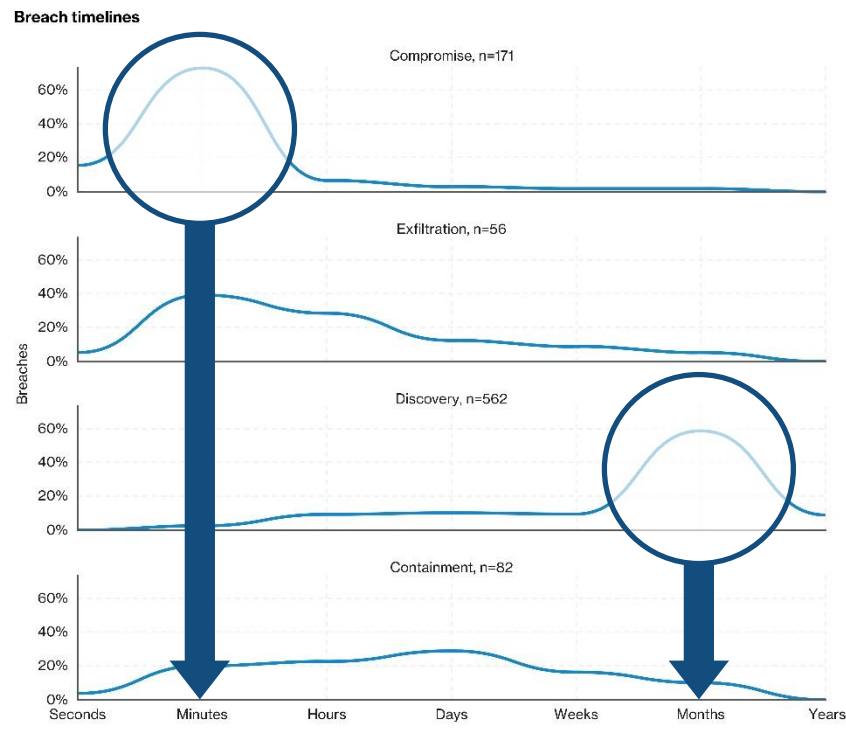


Figure 10. Time span of events

Unternehmen erkennen Hacks erst nach 197 Tagen



The screenshot shows the top navigation bar of the thyssenkrupp website with the logo and tagline 'engineering. tomorrow. together.'. Below the navigation bar, there are links for 'Unternehmen', 'Produkte', 'Investoren', 'Newsroom', and 'Karriere'. The main headline reads 'Cyberangriff auf thyssenkrupp'. A sub-headline states: 'thyssenkrupp ist Ziel eines massiven Cyberangriffs geworden. Die WirtschaftsWoche berichtet hierüber in ihrer aktuellen Ausgabe vom 9. Dezember 2016.'

Der Vorfall wurde etwa zwei Monate nach der Erstinfektion detektiert, als auf Systemen Fehlanmeldungen beobachtet wurden.*

Table 1: Breach Detection Gap Examples

Victim	Reported	Time to Discovery
Michaels Stores	Jan 2014	8 Months
Home Depot	Sept 2014	5 months
PF Chang's	July 2014	11 months ⁴
Sony	Nov 2014	~1 Year
Office of Personnel Management (OPM)	June 2015	~1 Year
Trump Hotels	Sept 2015	~1 Year
Undisclosed Mandiant client	2015	8.5 years

<https://www.thyssenkrupp.com/de/newsroom/datensicherheit/>

*https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf;jsessionid=D08643F7581FF177DC2D235F8AC2E801.1_cid360?__blob=publicationFile&v=4

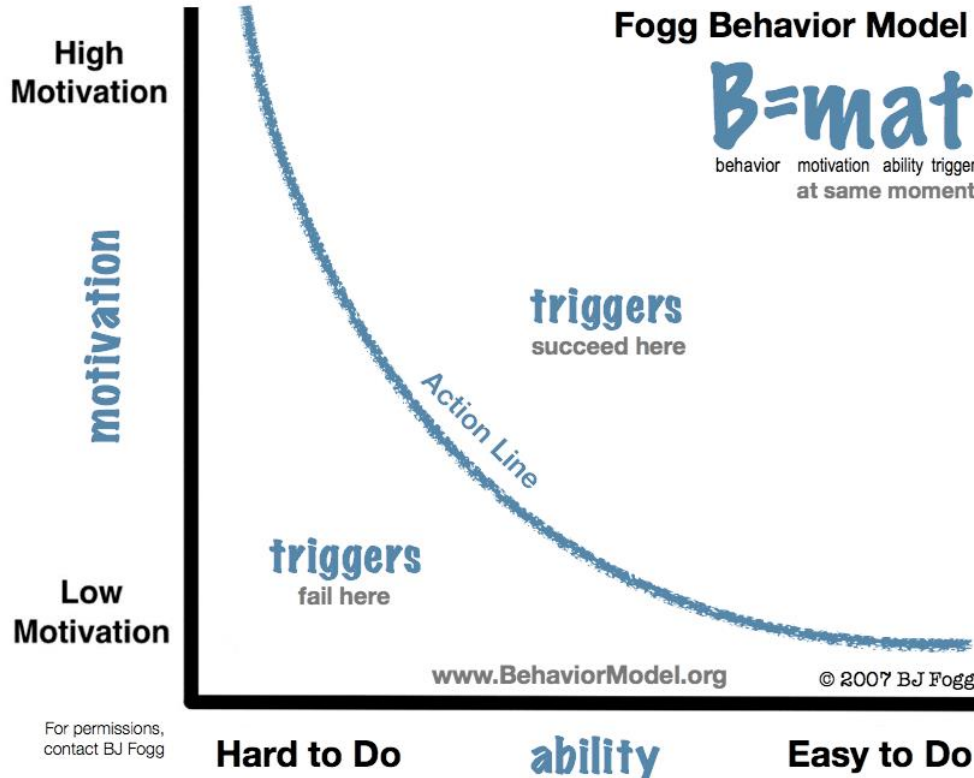
<https://www.infocycle.com/blog/2016/7/26/how-many-days-does-it-take-to-discover-a-breach-the-answer-may-shock-you>



Was passiert bei falschen Security-Einschätzungen im Flugzeug?



Der Mensch ist ein Gewohnheitstier



Kernfaktoren sind:

- Motivation
- Befähigung / Umsetzungsvermögen

Beispiel Passwörter

- Mindestens 8 Zeichen
- Läuft nach 90 Tagen ab
- Besteht aus min. 3 von 4:
 - GROSSBUCHSTABEN
 - Kleinbuchstaben
 - Zahlen
 - Sonderzeichen
- Die letzten 10 Passwörter dürfen nicht verwendet werden

$7,2 \times 10^{\text{hoch } 15}$

- Mindestens 12 Buchstaben

$3,9 \times 10^{\text{hoch } 20}$



DAU

PEBKAC - Problem zwischen Tastatur und Stuhl

Das schwächste Glied

„Anwender“

NOOB



Es muss einfach sein!



Einfache
Botschaften



Einfach
umzusetzen



Regelmäßig
geschult



Für Motivation
sorgen

Wie machen es Airlines

Inhalte festlegen

Wenige Themen

1



2

3

Trainings durchführen

Anschaulich



Erfolgskontrolle

Alle angeschnallt?



Was empfiehlt TO

Inhalte festlegen

Wenige Themen



Passwörter



Trojaner



Social Engineering

Trainings durchführen

Regelmäßig



Präsenz



Web Based

Erfolgskontrolle

Messung



Lob



Tadel

**Ihre
Mitarbeiter
sind besser
als jede
Firewall**



TOsecurity

Cyber Security von Anfang an.
security.to.com



Götz Weinmann
Bereichsleitung
TOsecurity Strategie

Tel. +49 711 88770-123
goetz.weinmann@to.com

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal / Stuttgart

Tel. +49 711 88770400
www.to.com
blog.to.com