Unternehmen im Fokus

Cybercrime wirkt da „wo es weh tut“

Kurzdarstellung aus einer polizeilichen Perspektive

Autor
und
Referent
© 2023

Kriminalhauptkommissar a.D.
Dirk Beerhenke
0163 1400 173
dirk@beerhenke.eu

Cybercrime ist en vogue

Ein Plan – Prävention härtet

Foto: Dirk Beerhenke

dirk@beerhenke.eu

Vita

α
01.10.1980

Ausbildung 1. Fachprüfung 2,5 Jahre

Streifendienst 6 Jahre

Straßenkriminalität – Zivilstreife 6 Jahre

Kriminalhauptmeister – Kfz-Diebstahl 1,5 Jahre

Studium 2. Fachprüfung, Dipl. Verwaltungswirt – 2 Jahre

Ermittler – Cybercrime 17 Jahre

Kriminalprävention – Cybercrime 7 Jahre

Dirk Beerhenke
62 Jahre alt
Pensionär

Ω
01.10.2022

dirk@beerhenke.eu

Kriminalhauptkommissar a.D.
Dirk Beerhenke

Polizeiliche Kriminalstatistik für Deutschland

	2022	2021	2019
Cybercrime gesamt	136.865	146.363	123.006

Viele Auslandsstraftaten werden hier nicht gezählt

Bitkom, e.V. Berlin, 31. August 2022: 84% aller Unternehmen betroffen …

Statistisches Bundesamt 2021: 3,4 Millionen rechtliche Einheiten

Dunkelfeldforschung: Vier von fünf Straftaten werden nicht angezeigt

Aufklärungsquote um 25 %

dirk@beerhenke.eu

ANZEIGE(n), weil

- Beobachtung der Kriminalität
- Deliktarten
- Umfang und Zusammensetzung des TV-Kreises
- Erkenntnisse für repressive und präventive Maßnahmen
- Organisatorische Planung
- Kriminologisch-soziologische Forschung

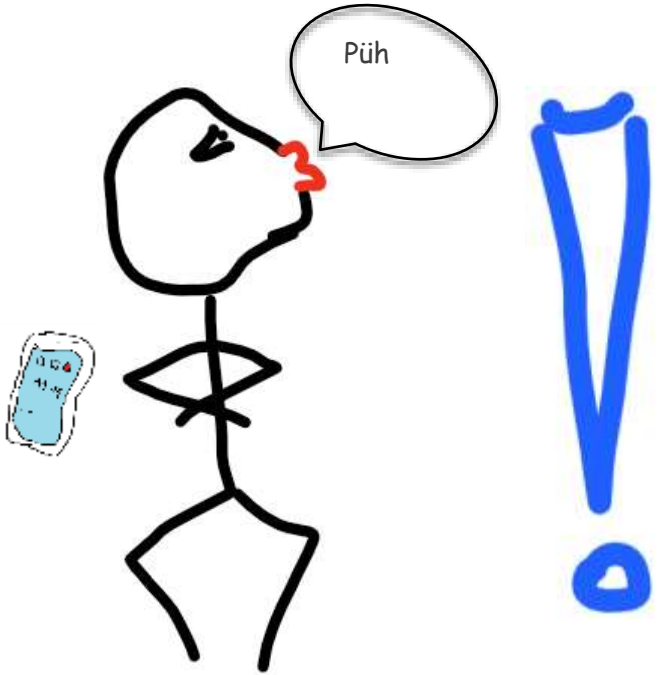
Strafanzeige erstatten:

Internetwache Polizei NRW

dirk@beerhenke.eu

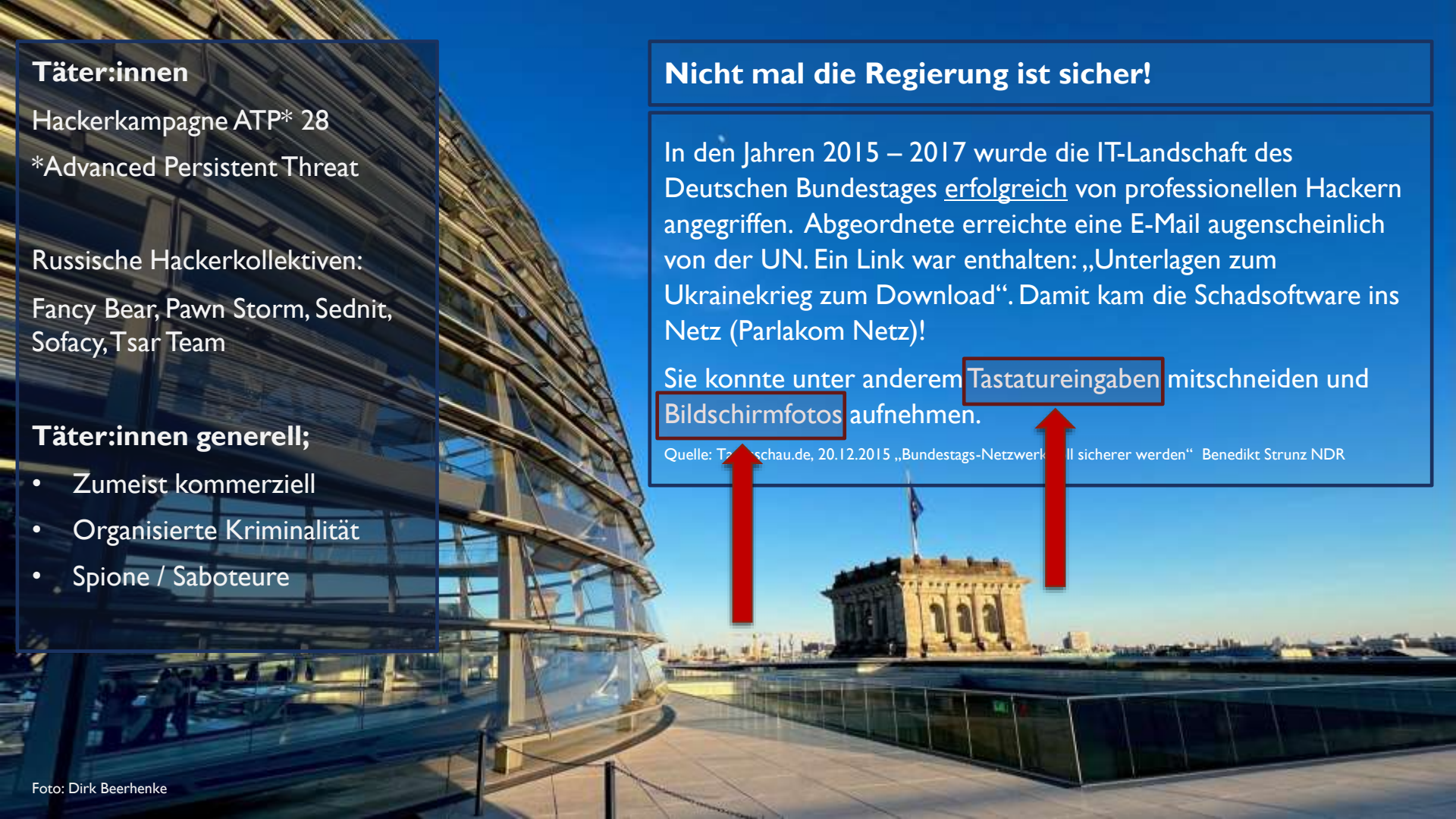
Einstellungssache

„Sollen *SIE* doch in meine Daten gucken….. - Ich habe nichts zu verbergen“



Zeichnung: Dirk Beerhenke

dirk@beerhenke.eu



Täter:innen

Hackerkampagne ATP* 28

*Advanced Persistent Threat

Russische Hackerkollektiven:

Fancy Bear, Pawn Storm, Sednit, Sofacy, Tsar Team

Täter:innen generell;

- Zumeist kommerziell
- Organisierte Kriminalität
- Spione / Saboteure

Nicht mal die Regierung ist sicher!

In den Jahren 2015 – 2017 wurde die IT-Landschaft des Deutschen Bundestages erfolgreich von professionellen Hackern angegriffen. Abgeordnete erreichte eine E-Mail augenscheinlich von der UN. Ein Link war enthalten: „Unterlagen zum Ukrainekrieg zum Download“. Damit kam die Schadsoftware ins Netz (Parlakom Netz)!

Sie konnte unter anderem Tastatureingaben mitschneiden und Bildschirmfotos aufnehmen.

Quelle: Ta[illegible]schau.de, 20.12.2015 „Bundestags-Netzwerk [illegible]ll sicherer werden“ Benedikt Strunz NDR

Foto: Dirk Beerhenke

Welche Daten können die Täter:innen erbeutet haben?

- Max.mustermann@muster.de
- Passwort: haubentaucher
- Amazon: haubentaucher1
- Tochter: Maxi Mustermann. Waldkindergarten….
- Einfamilienhaus mit Webcamüberwachung. Passwort: haubentaucher2
- Adresse: Musterstraße 6, Musterstadt
- Aufenthaltsorte (Geodaten)
- Ehefrau: Maria. E-Mail: maria.mustermann@muster.de, Tel. ….
- Mätresse in der Hauptstadt: Lola 26, Hornissenweg 888, E-Mail: lola26@muster.de, Tel. …
- Besuchte „Internetseiten“ …. alle ……
- Name und Erreichbarkeit der Security
- Kontakte der anderen Abgeordneten …. Wirtschaftsbosse …
- **Weitere Zugangsdaten, PINs, Onlinebanking** …….
- usw. …..

Foto: Dirk Beerhenke

doxing

Echt jetzt?

Bei mir auch!??

8-|

Foto: Dirk Beerhenke

Die Angreifer

A) Initial Access: E-Mail

B) Bekannte Schwachstellen (Exchange, FritzOS…) Schlampige Administration —— Warum ist das so?

Es ist zunächst unbekannt, wie lange sie im System sind!

Beute:

- Alle Zugangsdaten
- Kunden-, Patientendaten
- Zahlungsdaten
- Projekte / Entwicklungen……

Kontrolle

- Gebäudezugangssysteme
- Kameras, Mikrofone

Zu erwarten:

Womöglich nach Monaten des Wirkens: Verschlüsselung, Erpressung, Löschung, Veröffentlichung, Spionage ...

dirk@beerhenke.eu

Ransomware

Spürbar an Verschlüsselung und Erpressung

Hinweis:

Grundsätzlich keine Lösegeldzahlungen. Bestärkt das Geschäftskonzept der Banden!

Folge: Man ist wieder dran!

Prävention:

Backups!

dirk@beerhenke.eu

Spionage

Doku | ZDFinfo „Rote Spitzel – China und die Industriespionage“

- Gewaltiges Spionagenetz
- Seit 2006 wird unrechtmäßig erworbenes know how durch chinesische Patente reingewaschen

Russland und andere Staaten sind ebenfalls aktiv

- Autokratien
- Demokratien

Beute

Informationen von Spezialisten weltweit

- Einsetzen von „überzeugten“ Menschen der Zielfirma
- Einsetzen von Software

Hilfe

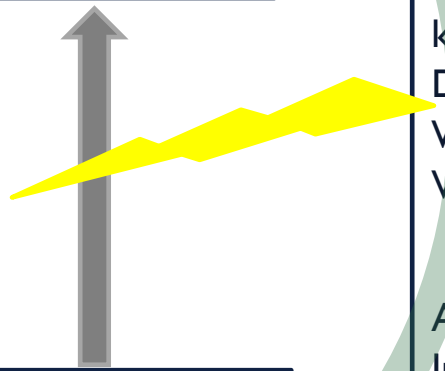
- Verfassungsschutz / Wirtschaftsschutz
- Bundesamt für Sicherheit in der Informationstechnik (BSI)

Foto: Dirk Beerhenke

dirk@beerhenke.eu

Sicherheit kostet Zeit, Geld und erfordert Disziplin

- Ungestört entwickeln
- hoher Ertrag
- Marktmacht



Ziele eines Unternehmens

Derzeit eingesetzte Schadsoftware legt den Betrieb bis zu vier Wochen lahm und katapultiert die Datenaktualität oft um Wochen zurück in die Vergangenheit

Anschlussmaßnahmen / Instandsetzungen dauern Monate!

Gelebte Prävention kann das Risiko deutlich vermindern

dirk@beerhenke.eu

Prävention – Verbesserung der Unternehmensresilienz

Hardware

- Gute und gut gewartete IT
- Pentests
- Standalone-Rechner
- GUTE Backups!

Fortbildung

- Fester Platz
- Mindestens jährlich
- Insbesondere mit Firmenleitung!

Notfallplan

- Analoge Dokumentation
- Evaluation
- In Fortbildung thematisieren

Experten wie

- BSI
- Wirtschaftsschutz
- Polizei Kriminalprävention
- Staatsanwaltschaft
- IHK
- Handwerks- / Handelskammer
- Verbraucherschutz
- digital-sicher.nrw

dirk@beerhenke.eu

Kriminalhauptkommissar a.D.
Dirk Beerhenke

Prävention - Vorbereitung auf den Notfall

Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheits-
vorfall

Was soll ich tun?

Notfall**ordner**

Papier, mindestens doppelte Ausführung

IT-Dienstleister

Gebäudezutritt (mechanisch!)

Bevollmächtigter, Notfallhandy

Firmenleitung, Notfallhandy

Alternativer Internetzugang, saubere Rechner aus der Reserve, **ohne** Firmennetz

Strafverfolgung

Andere wichtige Kontakte …… pp.

dirk@beerhenke.eu

Strafverfolgung - **IT-Vorfälle**!

Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen

Meine Empfehlung:

Suchen Sie VOR der Lage den Kontakt!

110

Verfassungsschutz **NRW**, Wirtschaftsschutz wirtschaftsschutz@im1.nrw.de

0211 871 2821

Ihre Kriminalpolizei *Ermittlungsdienststelle* = „Kriminalkommissariat Cybercrime“

Ihre Kriminalprävention: Kriminalkommissariat Kriminalprävention

dirk@beerhenke.eu

Wir sind für Sie da!

Die kriminalpolizeilichen Beratungsstellen in Ihren Polizeibehörden

„Polizei Kriminalprävention in Stadtname“

Dirk Beerhenke
Kriminalhauptkommissar a.D.
dirk@beerhenke.eu
0163 1400 173

ADVANT Beiten

IT-SICHERHEIT AUS RECHTLICHER SICHT

R+V ONLINE-EVENT IT-SICHERHEIT

DR. ANDREAS LOBER

IT-SICHERHEIT AUS UNTERNEHMENSSICHT

ADVANT Beiten

IT-SICHERHEIT AUS UNTERNEHMENSSICHT

QUIZ

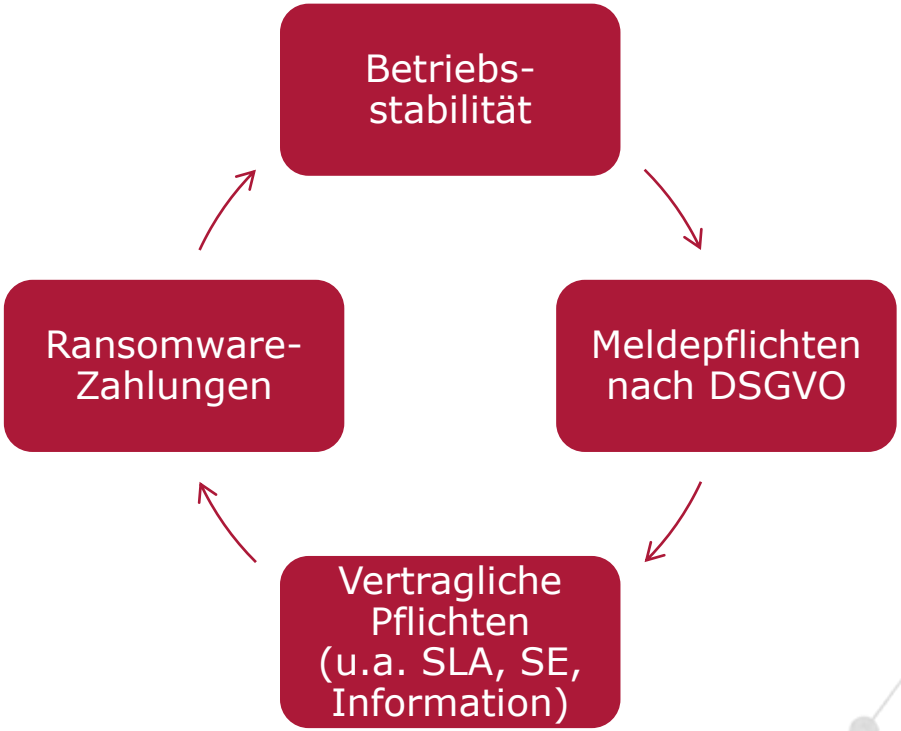
A: 72 Stunden

Antwort:

… nachdem das Datenleck bekannt wurde!

Es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt – bei einem hohen Risiko müssen auch die Betroffenen informiert werden!

IT-SICHERHEIT AUS UNTERNEHMENSSICHT



IT-SICHERHEIT AUS SICHT DER GESCHÄFTSFÜHRUNG

ADVANT Beiten

IT-SICHERHEIT AUS SICHT DER GESCHÄFTSFÜHRUNG

Haftung im Außenverhältnis

- grundsätzlich keine Haftung
- andere Sicht: OLG Dresden bei DSGVO-Verstößen

Strafbarkeitsrisiken

- TK-Geheimnis
- Ransomware

IT-SICHERHEIT AUS SICHT DER GESCHÄFTSFÜHRUNG

Haftung im Innenverhältnis

- Organe (Geschäftsführer, Vorstände) haften ggf. mit dem persönlichen Vermögen
- gegebenenfalls alle gemeinsam

Risikomanagement

- Analyse, Informations-, Organisations- und Überwachungspflichten
- Prävention (TOMs, Schulungen/Richtlinien)
- Reaktion, beseitigen, dokumentieren, melden, u.a. nach Art. 33 und 34 DSGVO
- Pflichtgemäße Prüfung der Notwendigkeit einer Versicherung (D&O, Cyber)

ADVANT Beiten

BEIJING | BERLIN | BRÜSSEL | DÜSSELDORF | FRANKFURT | FREIBURG | HAMBURG
LONDON | MAILAND | MOSKAU | MÜNCHEN | PARIS | ROM | SHANGHAI

ADVANT-BEITEN.COM

CYCO
Cyber Competence Center

Cyber-Prävention und Reaktion

Nikolaus Stapels

CyCo Cyber Comptence Center GmbH

Cyber-Policen benötigen hochwertige IT Dienstleistungen.

CyCo Cyber Competence Center in Hannover betreut 10 Versicherungsunternehmen im Bereich Cyber-Prävention und - Reaktion. Das Unternehmen wurde vom Gründer der SEC Consult Deutschland und der CYRISO Cyber Risk Solutions, Torsten Töllner und Nikolaus Stapels, gegründet.

- ISO27001 zertifiziert
- Schadenbearbeitung und Kundenbetreuung

CyCo Cyber Comptence Center GmbH

Incident Response Manager (IRM)

IT-Sicherheitsexperten, spezialisiert auf Sicherheitsvorfälle

und Angriffe auf Unternehmen / Organisationen

- 24/7/365 Bereitschaft
- Schnelle und effektive Reaktion auf Incidents, um den Schaden zu minimieren.
- Unterstützung der IT-Dienstleister der Versicherungsnehmer bei der Absicherung der IT-Systeme
- Unterstützung bei der Erstellung von Notfallplänen und Durchführung von Cyber-Übungen

Cyber Sicherheit betrifft jedes Unternehmen

Cyber-Security is much **more** than a **matter** of **IT**.

Viele erfolgreiche Cyber-Angriffe hätten vorab verhindert werden können. Viele Unternehmen Wissen jedoch nicht, wie die Kriminellen vorgehen und wie einfach es ist, einen Menschen zu hacken. Hier unterstützt CyCo zusammen mit Kooperationspartner die Unternehmen in Europa.

- CyCo Trap
- Schwachstellen Analysen (Penetrationtests)
- Präventionsdienstleistungen

CYCO
Cyber Competence Center

Im Schadenfall

Cyber Sicherheit betrifft jedes Unternehmen

Klassischer Schadensfall **eines** Gewerbekunden.

- Das mittelständische Unternehmen, Zimmerei Meisel GmbH, das einen Jahresumsatz von 2.600.000 € vorweist, wurde Opfer eines umfassenden Cyber-Angriffs.
- Alle digitalen Systeme, einschließlich Computerarbeitsplätze und Maschinensteuerungen, wurden verschlüsselt und sind somit vollständig lahmgelegt.
- Durch die seit Monaten bestehende Infiltration der Hacker sind nicht nur die primären Systeme betroffen, sondern auch die Datensicherungsmechanismen wurden sabotiert oder "infiziert", was eine einfache Datenwiederherstellung nahezu unmöglich macht.

CYCO
Cyber Competence Center

Ablauf bei einem Incident

01
Schadenmeldung

Die Schadenmeldung trifft via Telefon oder Mail ein

02
Erstkontakt

Erstkontakt mit dem VN. Erfassung von weiteren Informationen

03
Datenschutzvertrag inkl. Cloud

Zusendung Datenschutzvertrag. Freigabe für unsere Cloud um geforderte Daten hochladen zu können.

04
Prüfung der Daten

Die zugesandten Daten werden auf Vollständigkeit und Richtigkeit geprüft.

05
Analyse

Detailierte Analyse der bereitgestellten Daten.

06
Zwischenbericht

Die ermittelten Infos werden dem VN und der Versicherung zur Verfügung gestellt.

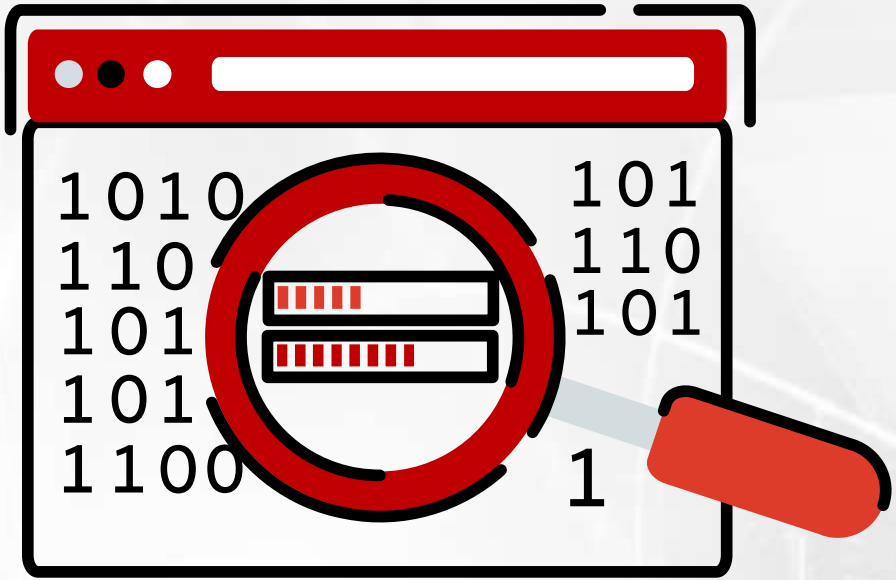
07
Weitere Analysen / Schlussbericht

Sollten weitere Tätigkeiten notwendig sein, werden diese mit dem VN und der Versicherung besprochen. Andernfalls wird der Schlussbericht erstellt.

CYCO
Cyber Competence Center

Prävention

Prävention



- Lücken vor dem Hacker aufdecken.
- Netzwerkausfallzeiten reduzieren
- Sicherheitsvorschriften einhalten
- In effiziente Sicherheits-maßnahmen investieren
- Image vom Unternehmen bewahren

Externer PenTest

Proaktive Cyber-Sicherheit

Bei einem Penetrationstest dringen wir von außen in Ihre IT-Systeme ein. So wie es ein Hacker täte. Unsere Tester sind bestens mit Angriffsmethoden vertraut. Sie suchen nach gängigen und exotischen Sicherheitslücken.

In einem umfangreichen Bericht informieren wir Sie über alle gefundenen Probleme und unterbreiten Vorschläge, wie diese behoben werden können.

CYCO
Cyber Competence Center

Prävention

Interner PenTest

Interne Sicherheit gewährleisten

Bei einem internen Penetrationstest geht man davon aus, dass man sich bereits auf den Systemen befindet. Es wird getestet, wie weit man mit den jeweiligen Rechten im Unternehmen kommt, ob man sich selber die Rechte aneignen kann und welcher Schaden angerichtet werden kann.

In einem umfangreichen Bericht informieren wir die Unternehmen über alle gefundenen Probleme und unterbreiten Vorschläge, wie diese behoben werden können.

CYCO
Cyber Competence Center

Prävention

Firewall und Antivirenschutz sind vergangenheitsorientiert.
Wenden Sie sich der Zukunft zu!

Wir legen präparierte Köder für die Hacker aus. Damit wird die Erkennung des Angreifers vereinfacht. Der Angriff wird frühzeitig erkannt, um eine eventuelle Betriebsunterbrechung zu vermeiden. Es erfolgt ein 24/7/365 Monitoring.

- Eine Falle schützt die Werte des Unternehmens
- Ständige Überwachung und im Bedarfsfall Alarmauslösung
- Forensische Analyse erleichtert

CYCO
Cyber Competence Center

Prävention

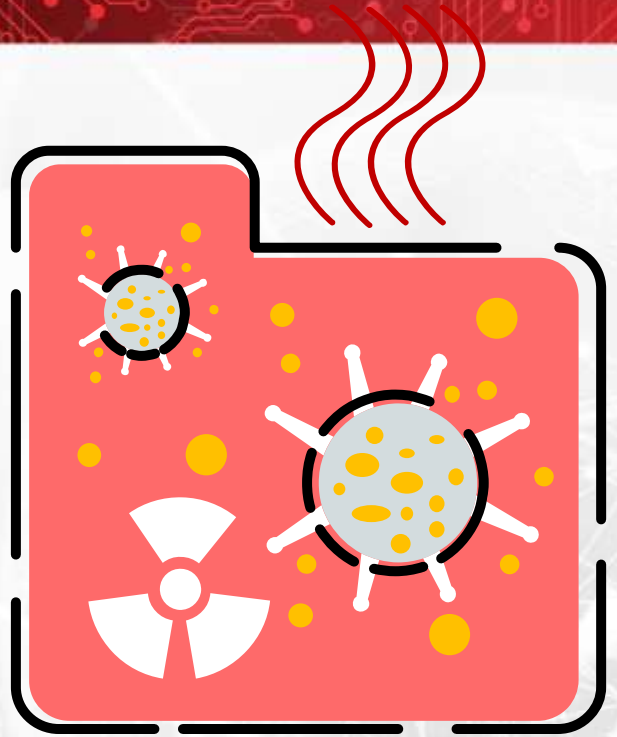
Unser Ansatz:

Der Angreifer ist **bereits** im System…

Der Angreifer wird auf eine Täuschumgebung weitergeleitet.
Dort kann dieser überwacht werden, ohne dass ein Schaden für das Unternehmen entstehen kann.

Für die Identifizierung werden Köder (Lures / Honeypots) ausgelegt, welche für Angreifer lukrativ scheinen.

Mit diesem Ansatz können Täter schnell identifiziert werden, bevor größere Schäden entstehen.



CYCO
Cyber Competence Center

Prävention

Der Hacker in der Falle…

Durch unser Monitoring-System können wir nun feststellen, was der Hacker im System sucht und wohin die Daten geschickt werden.

Der Versicherungsnehmer wird parallel telefonisch darüber informiert, dass sich ein Eindringling im System befindet.

CyCo beginnt sofort mit der Reparatur der Systeme und der Schließung der Sicherheitslücken.

Dadurch erhält der Kunde einen umfassenden Service des Versicherers, der in der Regel schneller den Eindringling identifiziert als der Kunde. Somit können durch die schnelle Reaktionszeit die Schadensquoten massiv gesenkt werden.

CYCO
Cyber Competence Center


thank you
CYCO
Cyber Competence Center