KRALOS

KRALOS CYBER SECURITY

Was ist wirklich gute Cyber Security?

Mehr Produkte = mehr Sicherheit?

Reichen Passwort, Firewall und Virenschutz?

Oder müssen wir Sicherheit grundsätzlich anders denken?

Cyber Security ist kein IT-Thema

KRALOS

- **Produktion**
- **Kommunikation**
- **Kundendaten**
- **Finanzen**
- **Lieferfähigkeit**
- **Reputation**

Wenn IT ausfällt, kann heute das Unternehmen ausfallen.

ANGRIFFSMUSTER

Wie denkt ein Angreifer?

Der Angreifer sucht nicht 100 Schwachstellen. Eine reicht.

- ✕ **Vergessenes System**
- ✕ **Schwaches Passwort**
- ✕ **Gefälschte E-Mail**
- ✕ **Veraltete Software**
- ✕ **Falsch eingerichteter Zugang**
- ✕ **Unaufmerksamer Mitarbeiter**

Der Angreifer muss nicht überall gewinnen. Das Unternehmen muss dagegen sehr viele Bereiche gleichzeitig schützen.

ANGRIFFSVERLAUF

Ein Angriff beginnt oft unspektakulär

1	2	3	4	5
Information sammeln	**Schwachstelle finden**	**Zugang bekommen**	**Ausbreiten**	**Schaden verursachen**
Webseite ansehen	*Mitarbeiter identifizieren*	*E-Mail-Adressen finden*	*Systeme ausprobieren*	*Einen Fehler entdecken*

Noch ist nichts Spektakuläres passiert. Das nimmt Cyberangriffen dieses Hollywood-Bild vom Hacker im dunklen Keller.

FALLBEISPIEL

Ein kleines Beispiel

Stellen wir uns ein Unternehmen mit 50 Mitarbeitern vor.

- ✓ Gute Firewall
- ✓ Virenschutz
- ✓ Sichere Passwörter
- ✓ Datensicherung
- ✓ Geschulte Mitarbeiter

Aber: Eine alte Anwendung wurde vergessen.

von außen erreichbar → seit Monaten nicht aktualisiert → der Angreifer findet sie

Das Grundproblem

Unternehmen denken häufig:

„Was können wir noch hinzufügen?“

Die bessere Frage lautet:

„Was kann ein Angreifer überhaupt erreichen?“

KOMPLEXITÄT

Viele Schutzsysteme lösen nicht automatisch das Problem

1. Mehr Systeme
2. Mehr Einstellungen
3. Mehr Meldungen
4. Mehr Verantwortung
5. Mehr mögliche Fehler

Komplexität kann selbst zum Risiko werden.

STRATEGIE

Erkennen oder verhindern?

Klassischer Ansatz

- Angriff passiert
- Angriff erkennen
- reagieren

Besserer Ansatz

- Angriff kommt
- Zugang begrenzen
- Angriff scheitert

Je später Sicherheit eingreift, desto größer kann der Schaden bereits sein.

Unterschied zwischen reagierender und vorbeugender Sicherheit

ANALOGIE

Ein einfaches Bild: Das Haus

Zugangskontrolle **Alarmanlage**

Ein sicheres Haus braucht nicht nur eine Alarmanlage.

Türen

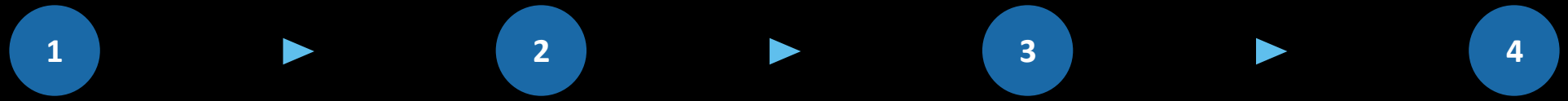
Schlösser

Fenster

Wände

Sicherheit muss früher beginnen

Sicherheit darf nicht erst nach dem Aufbau kommen.



Secure by Design

„Wir bauen ein System von Anfang an so, dass ein Angreifer möglichst wenig Möglichkeiten bekommt.“

Misstrauen kann etwas Positives sein

KRALOS

Nicht automatisch vertrauen.

- **Wer möchte hinein?**
- **Darf diese Person das?**
- **Darf dieses Gerät das?**
- **Darf diese Anfrage das?**
- **Ist das Verhalten plausibel?**

Erst prüfen. Dann erlauben.

Dieses Prinzip wird häufig „Zero Trust“ genannt.

Was passiert, wenn trotzdem etwas schiefgeht?

Fehler werden passieren.

Menschen machen Fehler.

Software enthält Fehler.

Neue Angriffsmethoden entstehen.

Gute Cyber Security fragt nicht nur:

„Wie verhindern wir Fehler?“

▶

„Wie begrenzen wir den Schaden?“

PRINZIPIEN

Gute Cyber Security in 5 einfachen Regeln

1	**Angriffsfläche verkleinern**	*Nur erreichbar machen, was wirklich erreichbar sein muss.*
2	**Zugänge konsequent prüfen**	*Nicht automatisch vertrauen.*
3	**Systeme voneinander trennen**	*Ein Problem darf nicht alles mitreißen.*
4	**Angriffe möglichst früh stoppen**	*Nicht erst reagieren, wenn Schaden entstanden ist.*
5	**Mit Fehlern rechnen**	*Systeme so bauen, dass ein einzelner Fehler nicht zur Katastrophe wird.*

Und der Mensch?

„Der Mensch ist die größte Schwachstelle.“

Ist das wirklich fair?

Menschen machen Fehler.

Menschen werden manipuliert.

Menschen stehen unter Zeitdruck.

Menschen können nicht jede Gefahr erkennen.

Gute Sicherheit darf nicht davon abhängen, dass Menschen niemals Fehler machen.

PERSPEKTIVWECHSEL

Woran erkennt man gute Cyber Security?

Man muss nicht fragen:

- ✗ Welche Firewall benutzen wir?
- ✗ Welchen Virenscanner haben wir?
- ✗ Wie viele Sicherheitsprodukte haben wir?

Sondern:

- ✓ Was kann von außen erreicht werden?
- ✓ Was passiert, wenn jemand hineinkommt?
- ✓ Wie weit kann sich ein Angreifer bewegen?
- ✓ Wie schnell erkennen wir einen Angriff?
- ✓ Was funktioniert weiter, wenn etwas ausfällt?
- ✓ Wie schnell können wir wieder arbeiten?

Dafür muss man kein IT-Experte sein.

FAZIT

Was ist also wirklich gute Cyber Security?

- ✗ nicht: Jeden Angriff erkennen zu können.
- ✓ Systeme so aufzubauen, dass ein Angriff möglichst wenig erreichen kann.

Sicherheit ist kein Produkt.
Sicherheit ist ein Prinzip.

KRALOS

DIGITALE SICHERHEIT GEHT UNS ALLE AN

Digitale Sicherheit sollte kein kompliziertes IT-Thema sein – sie geht uns alle an.

WEBOUNCER

Webouncer

Schutz für alle Web Anwendungen –
verhindert automatisierte Angriffe.

SHADOWKEY

Shadowkey

Sicherer Datentransfer.
Verschlüsselt, bevor die Daten Ihr Gerät verlassen.

PHISHING-GUARD

Phishing-Guard

Viren-Detektor für QR-Codes
– einfach sicher scannen.

Verstehen. Begrenzen. Schützen.

Fragen?