sure[secure]

Taktik, Verteidigung und Cyberabwehr

it-sa 2022, Nürnberg

IT-Security made with

Agenda

(1) Sie wurden also gehackt. Was nun?

(2) Ein Angriff aus dem Lehrbuch

(3) Vorbereitung auf Incidents

Sie wurden also gehackt...

Was nun?


DON'T
PANiC!

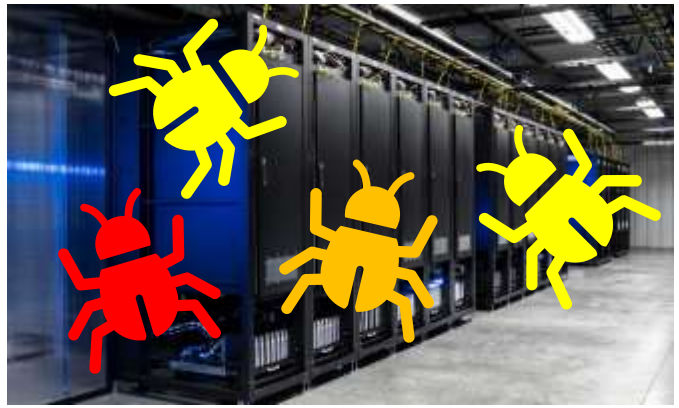
Sie wurden also gehackt… Und nun? Lösegeld zahlen?

Wie mit Ransomware und Vollverschlüsselung umgehen?

Soll ich bezahlen…?!

Nein!

1. Es gibt **keine Garantie**, dass Ihre IT hinterher wieder funktioniert.
2. Der Angreifer hat **weiterhin Kontrolle** über Ihre IT.
3. Das kriminelle System wird unterstützt und die **nächsten Angriffe finanziert**.



Ausnahme: Keine Backups von wichtigen Daten

Wie mit Ransomware und Vollverschlüsselung umgehen?

Ausnahme!

Zahlen, aber nur

- wenn **Daten nicht wiederherstellbar** sind,
- und diese für **den Fortbestand des Unternehmens** essenziell notwendig sind.

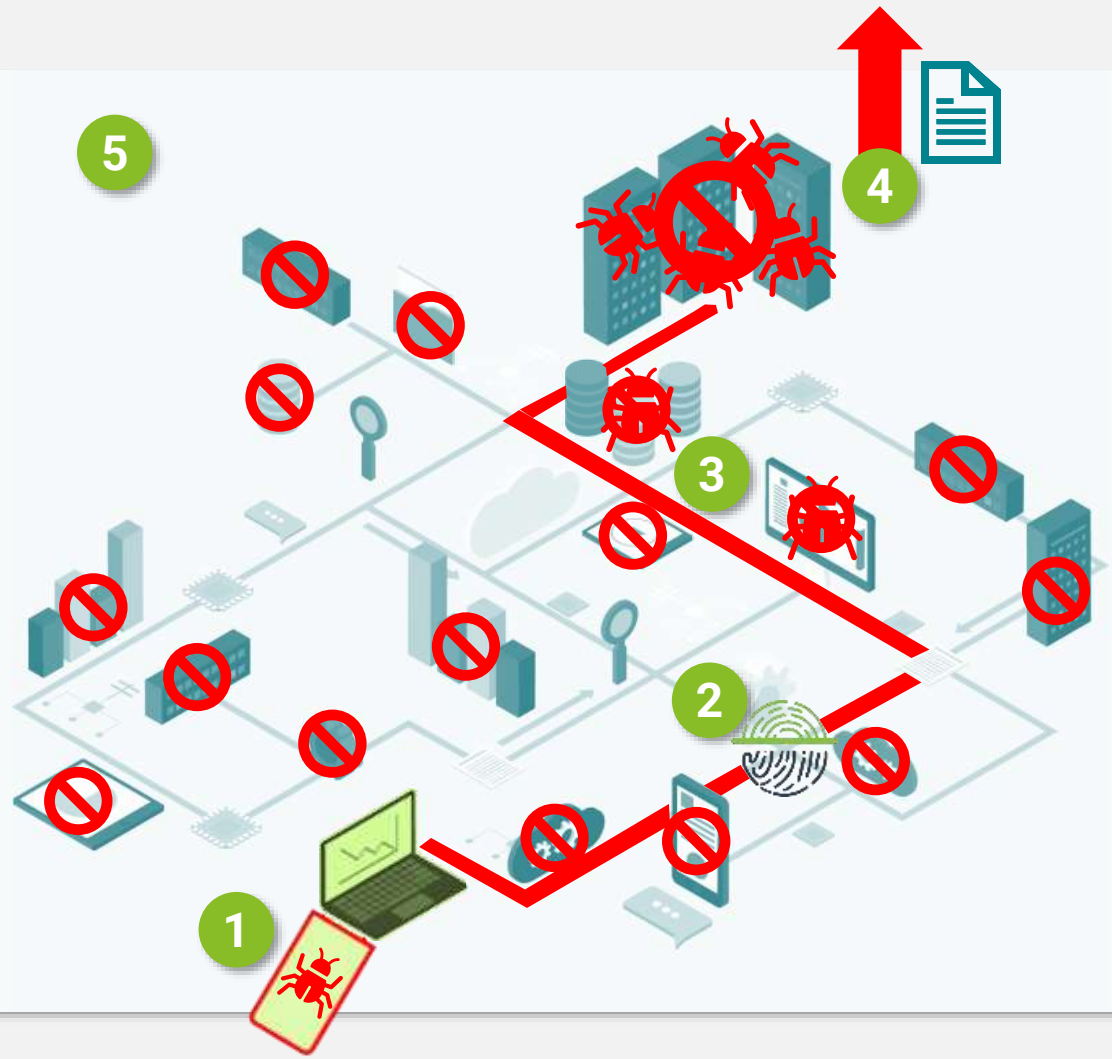
Ihre Daten werden auf jeden Fall monetarisiert!

Aus dem Lehrbuch: Cyberangriff

und daraus resultierende Schäden

Der Angriff beginnt bereits lange vor der Verschlüsselung

Prototypischer Angriffsverlauf vom Eindringen bis zum Verschlüsseln



1. **Eindringen**
   a) **Malware** wird unwissentlich ausgeführt
   b) **Schwachstelle** wird ausgenutzt
2. Erweiterung der **Berechtigungen** *(Mimikatz)*
3. Schaffen von **Persistenzen**
   - Angreifer nistet sich ein und …
   - … bewegt sich im Netzwerk (*PsExec*)
4. **Exfiltration** von Daten
5. Ausführen der **Verschlüsselung**

Ok…
Und wie kann ich das verhindern?

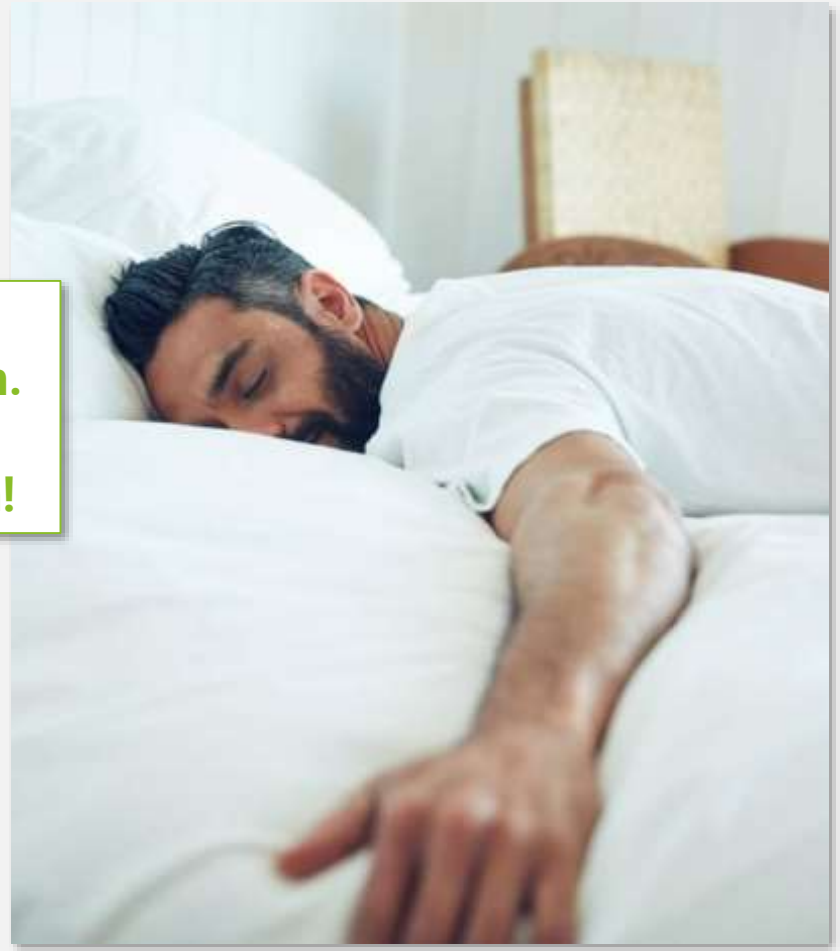
Wie kann ich überhaupt wieder schlafen?

Noch heute umsetzbare Sofortmaßnahmen für alle Unternehmungen

Wenn es zu einem Cyberangriff kommt, benötigen Sie schnelle und qualifizierte Hilfe

- Sorgen Sie für **Experten-Unterstützung** durch die Beauftragung eines externen Dienstleisters
  - Kurze Reaktionszeiten
  - Sichere Verfügbarkeit
  - Hohe Expertise und Erfahrung
- Schließen Sie eine **Cyber-Versicherung** ab
  - Abfederung des finanziellen Schadens
  - Deckung der Kosten der notwendigen Experten

Die beiden sollten voneinander wissen. Besser sogar: zusammenarbeiten!



Schaffen Sie eine Basis, um reaktionsfähig zu bleiben.

Nun will ich aber vielleicht auch wieder ruhig schlafen?

Echte Vorbereitung auf einen Incident durch vorausschauende Planung

Wenn es zu einem Cyberangriff kommt, müssen Sie sofort wissen, was zu tun ist. Sie brauchen einen Plan.

- Erstellen Sie einen **Incident Response Management Plan**!
  - Welche Prozesse sind geschäftskritisch?
  - Welche IT-Anwendungen sind für diese Prozesse notwendig?
  - Welche IT-Systeme brauchen diese IT-Anwendungen?
  - Was muss ich als erstes wieder aufbauen?
  - Wo sind meine Backups?
  - Wer kümmert sich um was?
  - Wie kommuniziere ich?

Wer weiß, was er im Falle des Falles tun muss, schläft ruhig.

Wie gut schlafe ich, wenn ich sicher bin, dass nichts passiert?

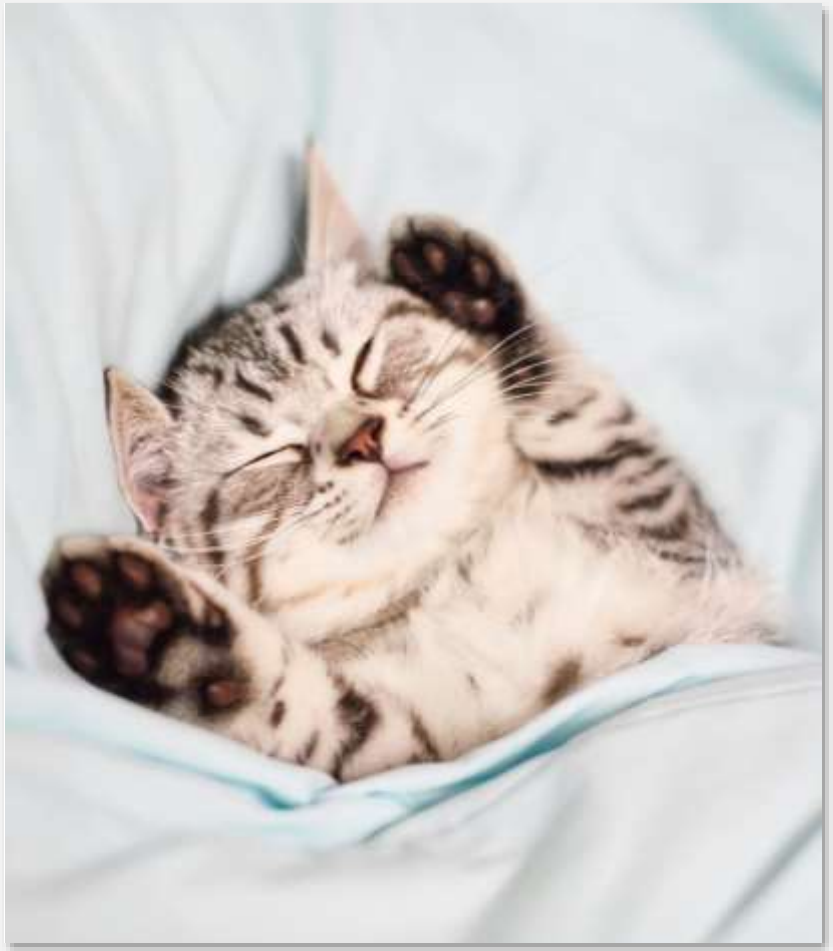
Mit einem SOC Incidents erkennen, bevor sie passieren

Sie müssen nicht auf einen Cyberangriff warten. Erkennen Sie ihn idealerweise, bevor er Schaden anrichtet.

- Bauen Sie ein **Security Operations Center** (SOC)!
  - Ein SOC überwacht ihre gesamte IT-Infrastruktur
  - Es erkennt Angreifer bereits beim Eindringen in Ihr System
  - Es warnt vor Schwachstellen
  - Es kann innerhalb kürzester Zeit reagieren und betroffene Systeme isolieren und den Angriff eindämmen

- Ein eigenes SOC ist zu teuer? Stimmt! Nutzen Sie daher einen Dienstleister und beauftragen Sie ein **SOCaaS**.

Wer weiß, dass ihm nichts passieren kann, schläft so richtig gut.




Fühlen Sie sich gut auf einen
Security Incident vorbereitet?

Bei der Wiederherstellung nach einem Sicherheitsvorfall können zwischen Tagen und Wochen Millionen Euro liegen!

Andreas Papadaniil,
CEO suresecure GmbH

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? → Besuchen Sie uns!
Booth 7-121

[s]

sure[secure]

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de


/suresecure.de


/suresecure-gmbh


/SuresecureD


/suresecuregmbh


/suresecure GmbH


/security horst

IT-Security made with