



**RELAX,
WE CARE**



700

Kunden



450

MitarbeiterInnen



16

Standorte



100%

Eigentümer geführt



142 Mio €

Umsatz 2020



100%

Menschlichkeit

NTS RELAX,
WE CARE

↑
LEIPZIG

REUTLINGEN

AUGSBURG

LINZ

WIEN

ROSENHEIM

SALZBURG

FRIEDRICHSHAFEN

INNSBRUCK

GRAZ

NTS SCHWEIZ

DORNBIRN

BOZEN/BOLZANO

KLAGENFURT

← **NTS NORTH AMERICA**

NTS CHINA →



NETWORK



SECURITY



SUPER SERVICES



COLLABORATION



DATA CENTER



SECURITY FIRST: SIND SIE SICHER, DASS SIE SICHER SIND?

29.09.2021 | ADV Konferenz | Villach



FRAGEN, DIE SICH UNSERE KUNDEN STELLEN



Wie kann ich mein Unternehmen gegen die **aktuellen Bedrohungen** schützen?



Was muss ich im **Notfall** tun?
Wie muss ich reagieren?

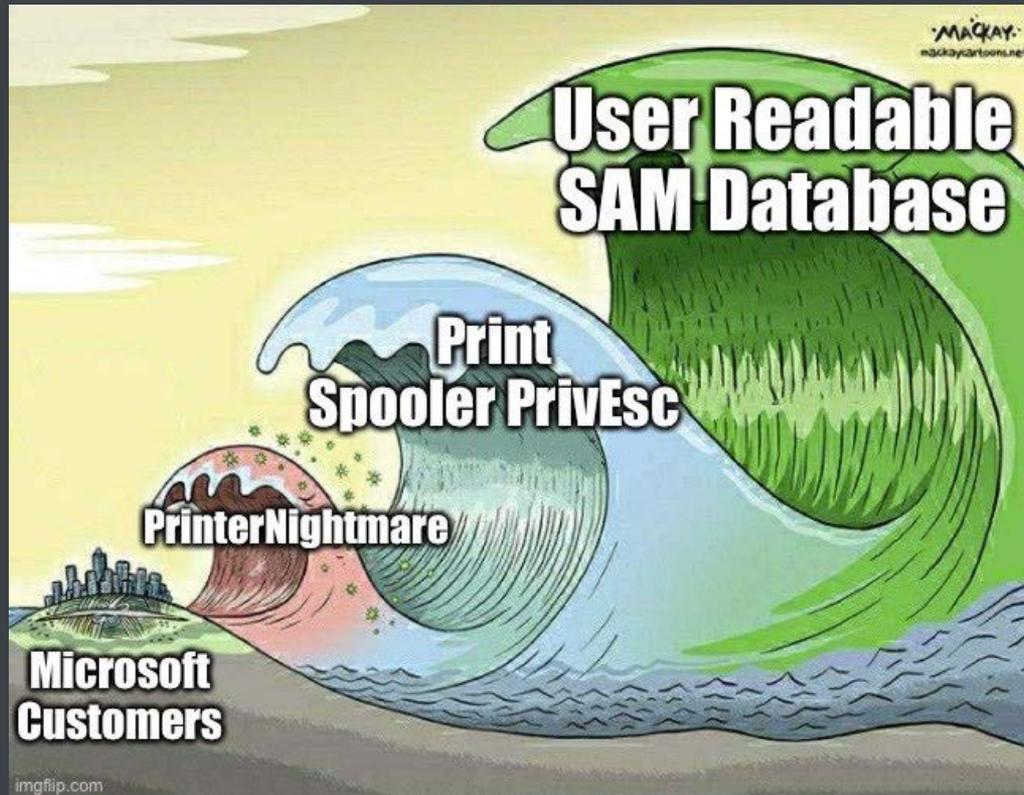


Wie finde ich raus,
wie und warum etwas passiert ist?



AKTUELLE BEDROHUNGEN

MICROSOFT SCHWACHSTELLEN



AKTUELLE BEDROHUNGEN



Microsoft Schwachstellen

Printer Nightmare
Print Spooler PrivEsc
User Readable SAM DB

Citrix (Shitrix)
Intel (CPU Issues →
Meltdown & Spectre)
OpenSSL (Heartbleed)

uvm.



Ransomware

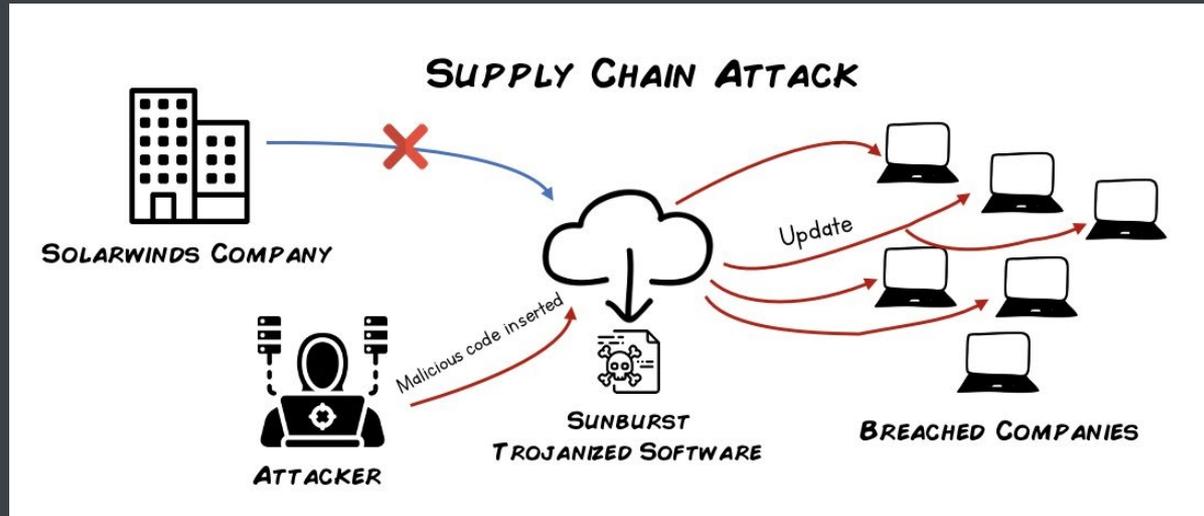
Schadprogramme, die
verschlüsseln

Erpressung / Lösegeld

Professionalisierung: RaaS

Daten-Veröffentlichung

SUPPLY CHAIN ATTACKS



AKTUELLE BEDROHUNGEN



Microsoft Schwachstellen

Printer Nightmare
Print Spooler PrivEsc
User Readable SAM DB

Citrix (Shitrix)
Intel (CPU Issues →
Meltdown & Spectre)
OpenSSL (Heartbleed)

uvm.



Ransomware

Schadprogramme, die
verschlüsseln

Erpressung / Lösegeld

Professionalisierung: RaaS

Daten-Veröffentlichung



Supply Chain Attacks

Kein direkter Angriff

Schwächstes Glied der
Kette wird genutzt

Software-Hersteller,
Dienstleister, Outsourcer

MASSNAHMEN



Microsoft Schwachstellen

ernst nehmen

Überblick behalten

Risiken richtig
einschätzen

Gesamt-Risiko gering
halten durch Vulnerability
Management



Ransomware

sensibilisieren

Angriffsfläche klein
halten: Segmentierung

MFA, PW Policies

Logging/SIEM für
Nachvollziehbarkeit



Supply Chain Attacks

proaktiv schützen

Secure Configs

„Least Privilege“ Prinzip

Logging/SIEM für
Nachvollziehbarkeit



HERAUSFORDERUNGEN

HERAUSFORDERUNGEN FÜR UNTERNEHMEN



Steigender Umfang und Raffinesse von Cyber-Angriffen



Zunehmend komplexere Umgebungen



Überwältigende Anzahl an Security Alarmen



Härtere Vorschriften und Strafen



Sicherheitsexperten sind schwer zu finden



NTS DEFENSE HILFT

NTS MANAGED SERVICE
SECURITY OPERATIONS



NTS DEFENSE SERVICE-ARCHITEKTUR

DEFENSE SERVICEBAUKASTEN

Vulnerability Management

Threat Detection Service | SIEM

NTS Defense Platform Betriebsführung

Customer Splunk ES

TDS | EDR

TDS | NTA

DEFENSE BACKEND

Splunk Mutter
SIRP Dashboard
Customer Service Reporting

ANBINDUNGEN

Threat Intel Feeds

Ticketing

Docu

NTS OC

Kunden

STARKES TEAM. STARKER SCHUTZ.



Vulnerability Management
hilft beim Absichern der
Infrastruktur und die
Angriffsfläche klein zu halten



Threat Detection Service hilft
während und nach dem Angriff
um zu Erkennen, was wann
warum passiert (ist)



VOR DEM ANGRIFF

ANGRIFF

NACH DEM ANGRIFF

NTS

**RELAX,
WE CARE**

NTS