SYNAXON

IT-SICHERHEITS FORUM 2024

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Marco Tessendorf

- Geschäftsführer der procado Consulting, IT- & Medienservice GmbH
- Senior Berater IT-Sicherheit / ISO27001 / BSI Grundschutz
- Dozent für Datenschutz an der IHK Potsdam
- Datenschutz- und Informationssicherheitsbeauftragter

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

„You´re fuc***d“ – reloaded!

1 Was ist denn hier los?

Wie erkennt man was eigentlich gerade passiert

2 Wo komm die den her?

Welche Angriffsvektoren wurden genutzt

3 Was soll man denn jetzt tun?

Erste Entscheidungen und Konsequenzen

4 Was hilft denn?

Erfolgreiche und nicht erfolgreiche erste und zweite Schritte

5 Was fehlte denn?

An was hätte man vorher denken sollen?

6 Wer soll das Bezahlen?

Kosten, Versicherungen und Fazit

01 Was ist denn hier los?

Erkenntnisgewinnung …

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Zeitliche Abfolge eines Angriffs

Angriffsversuch | Erfolg | Extraktion | Verschlüsselung | Erpressung | Veröffentlichung

Zeitfenster für Erkennung → **Fuc*** → Run → **Fuc***

Vorbereitung (Wochen – Monate) → Reaktion (Tage) → Eskalation (Std.)

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Offensichtliche Anzeichen

- Erscheinen einer Lösegeldforderung auf dem Bildschirm
- Sperrung des Zugriffs auf Dateien, Programme oder das gesamte System

Netzwerkaktivitäten

- Das Internet ist deutlich langsamer als sonst
- Verdächtige Netzwerkkommunikation mit unbekannten Servern oder hohen Datenvolumen

Probleme mit Sicherheitssoftware

- Warnmeldungen des Antivirenscanners
- Das Antivirenprogramm funktioniert nicht mehr oder lässt sich nicht aktualisieren

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Sonstige Anzeichen

- Programme stürzen häufiger ab oder arbeiten fehlerhaft
- Webbrowser lassen sich nicht mehr öffnen oder sind gesperrt
- Neue, unbekannte Software-Installationen tauchen auf

Ungewöhnliche Systemaktivitäten

- Erhöhte CPU- und Festplattenaktivität
- Der Computer arbeitet deutlich langsamer als gewohnt
- Unbekannte Programme oder Prozesse werden ausgeführt
- Der Mauszeiger bewegt sich ohne Zutun des Nutzers

In allen Fällen bei denen **procado** unterstützt hat
wären die Änderung von Anmeldedaten und Berechtigungen
bei sicherheitsrelevanten Konten
und ein Upload mit hohem Datenvolumen ins Internet erkennbar gewesen!

02 Wo kommen die denn her?

Eine nicht repräsentative Aussage …

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Erfolgreiche Ransomware-Gruppen nutzen verschiedene Wege, um in Systeme einzudringen

- Ausnutzung von Sicherheitslücken in (ungepatchter) Software
- Phishing-E-Mails mit schädlichen Links oder Anhängen
- Kompromittierung von Remote-Desktop-Protokollen (RDP)
- Supply-Chain-Angriffe über infizierte Dienstleister (Tools)

In allen Fällen bei denen **procado** unterstützt hat
kamen die Angriffen via E-Mail
und
trafen auf Konten mit zu hohen Rechten!

03 Was kann man tun?

Teilen und Herrschen …

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Welche Entscheidungen während eines Angriffs getroffen werden müssen

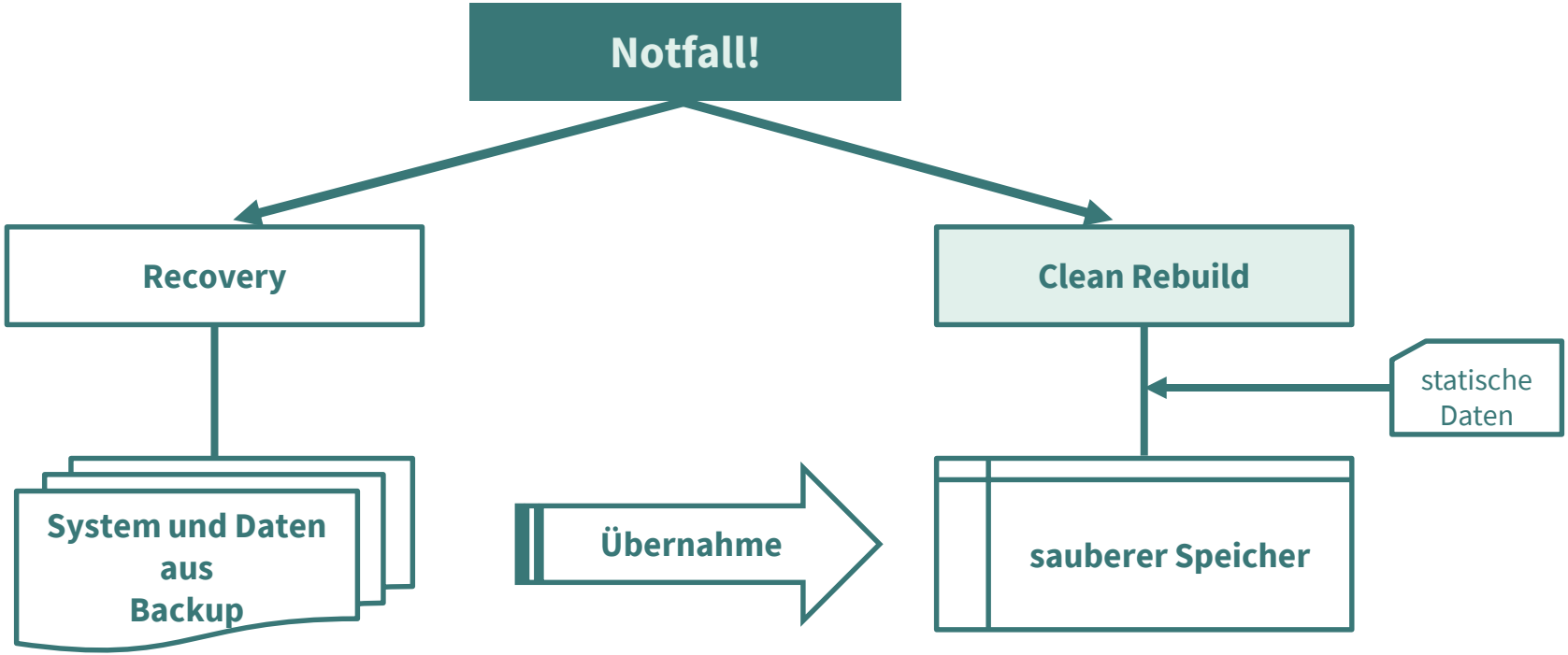
Grundlagen

- Ist es ein Angriff
- Ist der Schaden kalkulierbar
- Ist eine Wiederherstellung abschätzbar

Operativ

- Angriffsvektor bekannt / gebannt
- Forensik aktuell gewünscht

FINAL - Soll gezahlt werden?


Notfall!
Recovery
Clean Rebuild
statische Daten
System und Daten aus Backup
Übernahme
sauberer Speicher

04 Was hilft denn?

Erfolgreiche und nicht erfolgreiche erste und zweite Schritte …

Fakten

- Keine statischen Systemdaten offline vorhanden
- Rudimentäre Struktur und Funktionsdaten vorhanden
- Backup / Snapshot vermutlich vorhanden

operative Entscheidungen

- Wiederherstellung wird versucht
- Forensik kein primäres Ziel

Erfolgreiche erste operative technische Maßnahmen

- Kappung des Internetzugriffs
- Abschaltung aller Clients
- Abschaltung aller Server
- Priorisieren der Wiederherstellung kritischer Systeme

SYNAXON

Erfolgreiche operative technische Maßnahmen

- Netzwerksegmentierung
- Aufbau eines isolierten Recovery Bereiches
- Planung und Implementierung der Perimeter Absicherung

Erfolgreiche operative technische Maßnahmen

- Neuinstallation der Clients (Clean Master)
- Wiederherstellung der Server in Teilschritten aus vorhandenen Snapshots
- Teildatenimport aus Backup

procado
Consulting, IT- & Medienservice GmbH

SYNAXON

Schwierigkeiten während der Umsetzung

- Teilfunktionen der Netzes nicht nachvollziehbar
- Teilfunktion der Systeme und Schnittstellen nicht nachvollziehbar
- Teilfunktionen wegen fehlender Lizenzen nicht wiederherstellbar
- Datenverlust durch Differenz zwischen Snapshot / Backup und Realzeit

procado
Consulting, IT- & Medienservice GmbH

05 Was fehlte denn?

An was hätte man vorher denken sollen?

Fehlenden Informationen

- Keine strukturierte Dokumentation vorhanden
- Dokumentation und Speicherung von Lizenzinformationen
- Keine Dokumentation von Schnittstellen zu Kunden und Lieferanten (API)
- **Grundsätzlicher Mangel an IT Personal**
- **Wissensverlust durch Personalverlust!**

06 Wer soll das Bezahlen?

Kosten, Versicherungen und Fazit …

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Kosten durch einen Ransomware Angriff

- **Direkte Kosten (30%)**
  - Lösegeld
  - Arbeits- und Dienstleistungskosten der Wiederherstellung
  - Geräte- und Lizenzkosten

- **Indirekte Kosten (70%)**
  - Arbeitszeitausfall (~22 Tage –> 6 Monate)
  - Ausfall von Produktionskapazität
  - Effizienz- und Produktivitätsverluste (9 Monate)

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Cyberversicherung

Eigenschäden

- Wiederherstellung und Reparatur des IT-Systems
- Wiederherstellung oder Entschlüsselung von beschädigten Daten
- Austausch beschädigter Hardware
- Kostenübernahme des direkten Geldverlusts bei Datenklau bzw. Cyber-Diebstahl
- Informationskosten bei Datenschutzvorfällen
- Schäden durch Fehler von Angestellten und Mitarbeitern

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Cyberversicherung

Schäden an Dritten

- Begleichen des Schadenersatzes bei berechtigten Forderungen von Dritten
- Erstattung von Folgekosten (z. B. Umsatzeinbußen, Rufschädigung, Betriebsunterbrechung beim Kunden)
- Abwehr unberechtigter Forderungen (passiver Rechtsschutz)

SYNAXON

procado
Consulting, IT- & Medienservice GmbH

Fazit

Oberste Priorität hat die Verfügbarkeit betriebsrelevanter Daten

- Grundsätzliche Funktionsübersicht (wer macht hier was)
- Netztopologie intern (IP, VLAN, VPN, …)
- Zugangsdaten intern (Backup, Firewall, Switche, nicht AD Konten, IoT, Telefon, …)
- AD Struktur, AD Konten (Liste), OU,
- AD Gruppen und Rechte (Listen), GPO, Skripte
- Konzepte (Backup, Rechte, …)
- Zugangsdaten extern (Internet, Web, E-Mail Domäne, Cloud Anwendungen,…)
- Lizenzen

- **ACHTUNG bei Personalverlust**

Fazit

Grundlagen

- Bullet Proof Backupsysteme (pull nicht push)
- Training der Beschäftigten
- Rechtekonzept
- Notfallkonzept
- …
- Cyberversicherung

Fragen ?

Vielen Dank für eure Aufmerksamkeit

© procado Consulting, IT- & Medienservice GmbH

Marco Tessendorf
Warschauer Str. 58a
10243 Berlin

www.procado.de
LinkedIn Profil
procado Blog

SYNAXON