PITS 2016

Public-IT-Security

Forum II: Keine Chance für Ransomware

Wie kann Daten-Kidnapping verhindert werden ?

In Kooperation mit SAX.CERT Computer Emergency Response Team des Freistaates Sachsen

Erfahrungen mit Ransomware Vorfällen

Inhaltsübersicht

- Kurzvorstellung und CERT - Aufgaben und Tätigkeitsfelder
- Erfahrungen mit Ransomware-Vorfällen
- Lösungsansätze
- Und wenn es nun doch passiert?
- FAZIT

Referent
Kurzvorstellung

Uwe Hoppenz

- Seit 2010 beim Freistaat Sachsen beschäftigt
- Im Staatsbetrieb Sächsische Informatik Dienste (SID) verantwortlich für Informationssicherheit und Notfallvorsorge
- Leiter des SAX.CERTs
- Seit September 2016 Stellvertretender Leiter der Leitstelle für Informationstechnologie der sächsischen Justiz

CERT-Architektur

Begriffsbestimmung / Aufgaben

CERT ist die Abkürzung für
"**Computer Emergency Response Team**"
(Computer-Notfallteam)

- Nach dem Auftreten der ersten Computer-Würmer wurde das erste CERT gegründet (*USA / Carnegie Mellon University)*
- Erste CERTs in Deutschland:
  - *CERT des Deutschen Forschungsnetzes (DFN-CERT)*
  - *Universität Stuttgart*
- CERTs existieren sowohl in der Wirtschaft, im Finanzbereich, in der Forschung und Lehre, aber auch im Behörden- und Regierungsumfeld (*CERT-Bund*)
- Das Landes-CERT in Sachsen (SAX.CERT)
  - 2013 gegründet
  - im Staatsbetrieb Sächsische Informatik Dienste (SID) angesiedelt

SAX.CERT
Computer Emergency Response Team des Freistaates Sachsen

CERT-Architektur

Aufgaben / Strukturierung

Aufgabenbereiche:

- **Präventive Aufgaben** – *Vorbeugen*
  - Erkennung und Reaktion auf Angriffsszenarien, Vorfälle und Sicherheitslücken.
- **Reaktive Aufgaben** – *Reagieren*
  - Reaktion auf Angriffe, Vorfälle und Probleme.
  - Die Entstehung größerer Schäden sowie die Ausbreitung der Vorfälle soll dabei verhindert werden.
- **Security Quality Management** – *Verbessern*
  - Verbesserung der Sicherheit und des Risikomanagements.

Ransomware
Erfahrungen mit Vorfällen

Ransomware ist nicht neu!

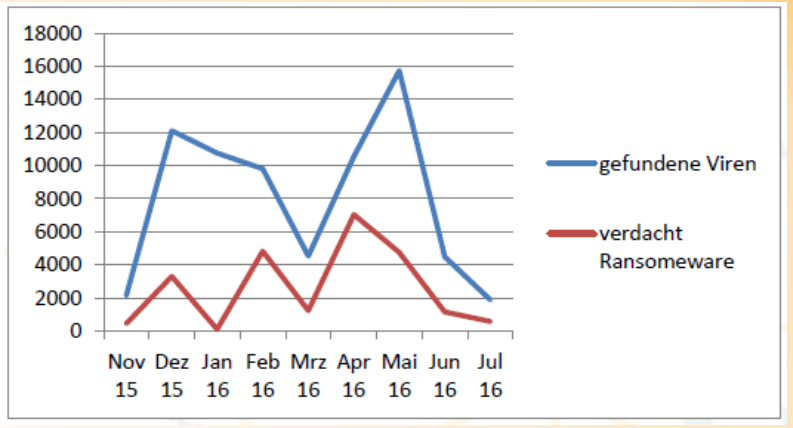
Erste Ransomware-Viren gab es bereits 1989 vor der Internet-Ära !

- **Auf Grund von Maleware/Crimeware-Baukästen starke Verbreitung**
  - *Einfache Erstellung*
  - *SLA für Betreuung!*
  - *Sehr gutes Verhältnis zwischen Aufwand und Gewinn*
- **Hype im laufenden Jahr:**
  - *Locky*
  - *Tesla Crypt*
  - *Cerber*
  - ***Neu:** Kryptotrojaner für OS X und Smartphones*

(über Security-Apps mit Sicherheitslücken)

Ransomware
Erfahrungen mit Vorfällen

Statistik



- Anstieg nach Aufkommen entsprechender Erfolgsmeldungen von Locky (12/2015)
- DHL-Mails und Bewerbungen (02/2016)
- Peak mit Tesla Crypt in allen Varianten (02-04/2016)
- Erstes Entschlüsselungs-Tool (06/2016)
- CERBER-Welle (05-06/2016)
- Abschwächung nach Veröffentlichung von Schlüsselmaterial und Tools im Juli

Wir befinden uns nur in der Ruhe zwischen zwei Stürmen

Ransomware
Erfahrungen mit Vorfällen

Statistik

- **Vorfälle im Einzelnen:**
  - Von Dezember bis Juli monatlich Vorfälle
  - Mehrere Wellen
  - Alle Fälle zeitig erkannt und nur wenige Rechner und Laufwerke betroffen
  - mittels Backup mit durchschnittlich einem Tag Verlust wiederhergestellt!
  - Keine Zahlung erfolgt!

Bisher Glück gehabt !!!!

Ransomware
Erfahrungen mit Vorfällen

Beispiele die das Leben schreibt:

- **Der Klassiker:**
  - *Alles sicher gemacht und jeden Mitarbeiter sensibilisiert, aber…*
  - *Die Azubis haben Zugriff auf ihre Web-Mailer am Arbeitsplatz-PC*
  - *Als sich der Anhang beim Ersten nicht öffnet, schickte er die Mail seinem Kumpel….*
- **Die Personalabteilung:**
  - *Intensive Sensibilisierung und Schulung*
  - *Mitten in einer großen Bewerber-Runde…*
  - *… und eine Bewerbung war eben doch nicht die Richtige*

Ransomware
Lösungsansätze

Prinzipiell:

- Die Cybercrime-Gemeinde schläft nie…
- Deshalb permanente Verbesserung ihrer Maßnahmen notwendig
- Mischung aus einer Vielzahl von technischen und organisatorischen Maßnahmen notwendig
- Beginn ist immer die Sensibilisierung

Ransomware
Lösungsansätze

Technische Ansätze:

- Alle bisherigen Sicherheitsmaßnahmen behalten weiter Gültigkeit (Firewall, Proxy, AV-Scanner, IDS etc.)

- Rechtevergabe auf Shares kritisch überprüfen:
  - Wo sind wirklich Schreibrechte notwendig?
  - Muss der Nutzer Zugriff auf diese Freigabe haben?

→ **Wo ein Trojaner nicht hinkommt und wo er nicht schreiben kann, kann er auch keinen Schaden anrichten!**

Sie werden staunen, wie viele Freigaben erreichbar sind und was mancher Nutzer für Rechte besitzt

Ransomware
Lösungsansätze

Technische Ansätze:

- **Backup-Strategie auf den Prüfstand**
  - Snapshot-Technologien
  - Mehr Lebenszyklen
- **Restore-Test**
  - Steht auf dem Band wirklich das, was ich erwarte?
  - Bekomme ich die Daten in einer akzeptablen Zeit wieder hergestellt?

Ransomware
Lösungsansätze

Technische Ansätze:

- **patchen aller Systeme**
  - Virenscanner Signaturen *(minimal stündlich bei zentralen Systemen)*
  - Schwachstellen-Patche umgehend einspielen
  - Nicht nur bei zentralen Systemen sondern auch bei allen Arbeitsplätzen

Ransomware
Lösungsansätze

Organisatorische Ansätze:

- **Sensibilisierung**
  - Permanente Sensibilisierungsmaßnahmen
  - Lebendige Beispiele → *Phishing-Tests*
  - Klärung, was dem Angestellten passiert, wenn er der Auslösende ist → *hoffentlich nichts allzu Schlimmes!?*

Ransomware
Lösungsansätze

Organisatorische Ansätze:

- **Prüfung der Prozesse**
  - Zeit ist der wichtigste Faktor beim Treffer
  - Sind alle Melde- und Eskalationswege bekannt
    → *vor allem auch beim Nutzer?*
  - Test der Abläufe → *Papier ist geduldig*
  - Meldung auch an andere Behörden, CERTs, Sicherheitsorganisationen bedacht?

Ransomware

Und wenn es doch passiert?

Schnelligkeit ist der wichtigste Faktor

- Betroffene Systeme separieren / vom Netz trennen
- Netzwerks-Laufwerke trennen
- Info an alle möglichen Betroffenen
- Schadensumfang bestimmen
- *Sicher stellen, dass Verbreitung eingegrenzt ist*

Ransomware

Und wenn es doch passiert?

Wiederherstellung initiieren

- Arbeitsplatzsysteme ersetzen
- Daten aus Backup einspielen
- Datenverlust bestimmen
- Eventuell Entschlüsselungs-Tools einsetzen

Ransomware

Und wenn es doch passiert?

Niemals Lösegeld zahlen !!!

- Firmen sind oft geneigt das Lösegeld zu zahlen um Image-Verluste zu umgehen
- Jede Zahlung motiviert Nachahmer
- Entschlüsselungs-Tools nutzen
- Immer Strafanzeige !!!

Keine Chance für Ransomware!

Fazit / Ausblick

- Ihre Abwehr muss aus einer Kombination von technischen und organisatorischen Maßnahmen bestehen
- Sensibilisierung, Sensibilisierung, Sensibilisierung
- Backup und strikte Leserecht-Vergabe auf Shares
- Systeme Patchen
- **KEINE Lösegeldzahlung !!!**

Jede Zahlung motiviert die Täter!

FRAGEN?

Uwe Hoppenz

Telefon (+49) (0351) 446 18010

E-Mail:
uwe.hoppenz@lit.justiz.sachsen.de

Sie finden das SAX.CERT unter:
www.cert.sachsen.de