TEFO 2021

KRYPTO-TROJANER: ANATOMIE EINES SUPER-GAUs

Mark Semmler

INHALT DER FOLIEN

- Auf den nächsten Seiten wird die Anatomie einer Ransomware-Attacke dargestellt, unterteilt einzelne Kapitel:
  - 1. Akt: Low-Level-Attacke mit der Gießkanne
  - 2. Akt: Aufbau eines Brückenkopfes
  - 3. Akt: Attacke gegen die gesamte Domain
  - 4. Akt: Angreifer hat freies Spiel
- Anschließend wird gezeigt, wie man sich vor Ransomware schützen kann...
  - Schutz für Klein- und Kleinstunternehmen
  - Schutz bei höheren Sicherheitsanforderungen
- ...und was man sich im Falle eines Falles tun kann/sollte.
  - Konkretes Verhalten bei Ransomware-Attacken

1. AKT:
LOW-LEVEL-ATTACKE MIT DER GIEßKANNE
(DER ALLTÄGLICHE WAHNSINN)

Mark Semmler

INITIALER ANGRIFF: GIESSKANNEN-PRINZIP

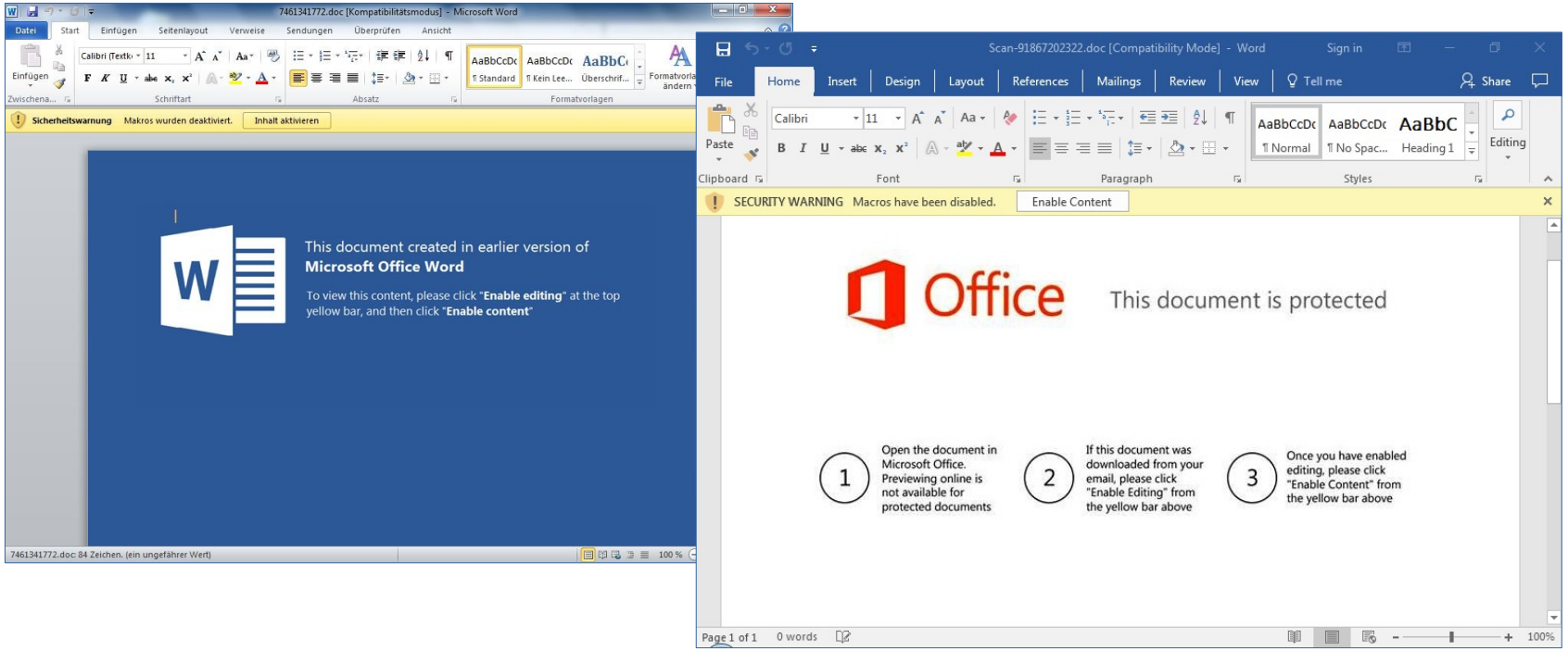
- Ransomware-Gruppen attackieren in aller Regel Unternehmen im ersten Schritt über einfache, wohl bekannte Wege:
  - Platz 1: Schadsoftware via E-Mail-Attachments
  - Platz 2: Raten von Passwörtern
  - Platz 3: Nutzen von ausgespähten Zugängen
  - Platz 4: Exploits
  - Platz 5: Vertrauenswürdige Kanäle
- Diese Angriffe sind Mengen- und Massenangriffe. Sie sind in aller Regel nicht speziell gegen ein Unternehmen gerichtet.

PLATZ 1: SCHADSOFTWARE VIA E-MAIL

- Mit weitem Abstand sind verseuchte E-Mail-Anhänge der Angriffsvektor Nr. 1.
  - MS Office-Dokumente mit eingebetteten Makros (> 95%)
    - MS Word (mit Abstand am häufigsten)
    - MS Excel (nicht selten)
    - MS Powerpoint (gelegentlich zu beobachten)
  - PDF mit eingebetteten Exploits gegen Adobe Acrobat Reader (selten)
  - sonstige (Anteil verschwindend gering, < 1%)
- Absender, Empfänger, Betreff und Text der E-Mails werden dabei auf Basis erbeuteter Mails erstellt, um eine höhere Klickrate zu erreichen.

BEISPIEL: VERSEUCHTE WORD-DOKUMENTE

- Nach dem Doppelklick werden die Opfer ggf. durch das Dokument dazu aufgefordert, die Makros („aktive Inhalte“) freizuschalten.



PLATZ 2: RATEN VON PASSWÖRTERN

- Die Angreifer versuchen Benutzernamen und Passwörter von IT-Systemen zu erraten, die aus dem Internet erreichbar sind.
- Besonders im Fokus: Remote-Desktop-Lösungen
  - Fernwartungssoftware
  - RDP
  - CITRIX
  - …
- Andere Dienste sind seltener im Fokus (z. B. CMS, SSH, …).
- Besonders erfolgreich, wenn Usernamen auf dem Login-Screen angegeben sein bzw. gewählt werden können und/oder sie einfach erraten werden können.

PLATZ 3: NUTZEN VON AUSGESPÄHTEN ZUGÄNGEN

- Die Angreifer versuchen Benutzernamen und Passwörter von IT-Systemen zu erraten, die aus dem Internet erreichbar sind.
- Besonders im Fokus: Remote-Desktop-Lösungen
  - Fernwartungssoftware
  - RDP
  - CITRIX
  - …
- Besonders erfolgreich, wenn Usernamen auf dem Login-Screen angegeben sein bzw. gewählt werden können und/oder sie einfach erraten werden können.

PLATZ 4: EXPLOITS

- Einzelne Gruppen suchen zielgerichtet nach IT-Systemen mit wohl bekannten Sicherheitslücken.
- Unter anderem wurden bereits die folgenden Verwundbarkeiten aktiv ausgenutzt:

PLATZ 5: VERTRAUENSWÜRDIGE KANÄLE

- Zahlenmäßige selten wird Ransomware über vertrauenswürdige Kanäle eingeschleppt.
- Wenn Ransomware-Gangs einen IT-Dienstleister übernommen haben, nutzen sie häufiger dessen Infrastruktur (VPN-Zugänge und/oder sonstige Fernwartungszugänge), um die Kunden des Opfers zu infizieren.
- In einzelnen spektakulären Fällen haben Ransomware-Gangs es geschafft, ihre Schadsoftware in reguläre Anwendungssoftware unterzubringen.
  - Beispiel: VSA (Virtual System Administrator) von Kaseya

PRAXIS: FALL 2020-03 – INITIALER BEFALL

- Ablauf:
  - Der Nutzer arbeitete als lokaler Administrator auf seinem privaten Rechner (Windows 7), tätigte einen Doppelklick auf den verseuchten Anhang einer Mail (DOCX) und gab die aktiven Inhalte frei.
- Ursachen:
  - Der Mitarbeiter erkannte die Mail nicht als gefährlich.
  - Der Virenscanner (Windows Defender) erkannte die Schadsoftware nicht.
- Verstärkender Faktor:
  - Der Mitarbeiter arbeitete als lokaler Admin auf seinem privaten Rechner.

PRAXIS: FALL 2020-08 – INITIALER BEFALL

- Ablauf:
  - Ein Unternehmen erhielt per E-Mail eine Warnung von einem ihrer IT-Dienstleister:
    - „Es ist unter Umständen möglich, dass Ihre IT von einer Sicherheitslücke betroffen sein könnte.
      Als Vorsichtsmaßnahme empfehlen wir, die Server in Netzwerk zeitnah auf folgende Anzeichen für ein mögliches Problem zu untersuchen: (...)“
  - Das Unternehmen nahm die Warnung aufgrund der schwammigen Formulierung zunächst nicht ernst. Ein Administrator fragte einige Tage später beim IT-Dienstleister nach und es stellte sich heraus, dass der IT-Dienstleister massive Probleme mit Ransomware hatte.
  - Das Unternehmen kappte sofort sämtliche Internetverbindungen, durchsuchte die IT und fand die Angreifer, bevor sie Daten verschlüsseln konnten.
- Ursachen:
  - Der IT-Dienstleister besaß VPN-Verbindungen zu seinen Kunden, die von den Angreifern genutzt werden konnten.
- Verstärkender Faktor:
  - Die VPN-Verbindungen konnten jederzeit (also ohne Freigabe durch die Kunden) genutzt werden.
  - Der IT-Dienstleister besaß Administrationsrechte auf den Zielsystemen und speicherte die dazugehörigen Passwörter im Klartext.

2. AKT:
AUFBAU EINES BRÜCKENKOPFES
(GEKOMMEN UM ZU BLEIBEN)

PRAXIS: FALL 2020-12 - EINNISTEN

- Ablauf:
  - Der Nutzer arbeitete als lokaler Administrator auf seiner Workstation (Windows 10), tätigte einen Doppelklick auf den verseuchten Anhang einer Mail (DOCX) und gab die aktiven Inhalte frei.
  - Auf dem initial infizierten IT-System wurde ein PowerShell-Script „pld“ („payload“?) heruntergeladen und ausgeführt.
    - Sammeln und melden verschiedener Systeminformationen.
    - Umgehen von UAC via Win32 API GetLongPathName (Methode 52 von https://swapcontext.blogspot.com/2020/10/uacme-35-wd-and-ways-of-mitigation.html).
    - Download des Tools „Defender Control“ (siehe https://www.sordum.org) und Abschalten des Windows Defenders.
    - Download und Installation von Poison Ivy RAT (RAT = Remote Access Tool).
    - Download und Etablieren eines PowerShell-Scripts mit Namen „syscheck“ via Autorun.
  - Script „syscheck“ (wird nach jedem Reboot ausgeführt):
    - Abschalten des Windows Defenders via „Defender Control“.
    - Prüfen, ob Poison Ivy RAT aktiv/installiert ist. Ggf. Download und Starten/Installieren von Poison Ivy RAT.
- Ursachen:
  - User arbeitete als lokaler Admin.
  - Als Virenscanner wurde allein Windows Defender eingesetzt.

PRAXIS: FALL 2020-03 – CLIENT AUSSPÄHEN

- Ablauf:
  - Angreifer betritt das System via RAT.
  - Download und start von Script „harvester“.
    - Download des Tools „WebBrowserPassView“ (siehe https://www.nirsoft.net/utils/web_browser_password.html) und Auslesen aller in den Browsern der lokalen Nutzer gespeicherter Passwörter. Speichern der Passwörter als txt-Datei in einem temporären Ordner.
    - Suche nach *.pst-Dateien sämtlicher lokaler Nutzer und verlinken der Dateien im temporären Ordner.
  - Angreifer überträgt die gesammelten Informationen auf sein System.
- Ursache:
  - Kein Master-Passwort im Browser gesetzt.
- Verstärkende Faktoren:
  - Vermischung zwischen privater und geschäftlicher Nutzung.
    - Passwörter für CITRIX waren im Browser des Users gespeichert.
    - Geschäftlicher Mailaccount wurde von privatem System abgerufen.

PRAXIS: FALL 2020-03 – DOMAIN ADMIN

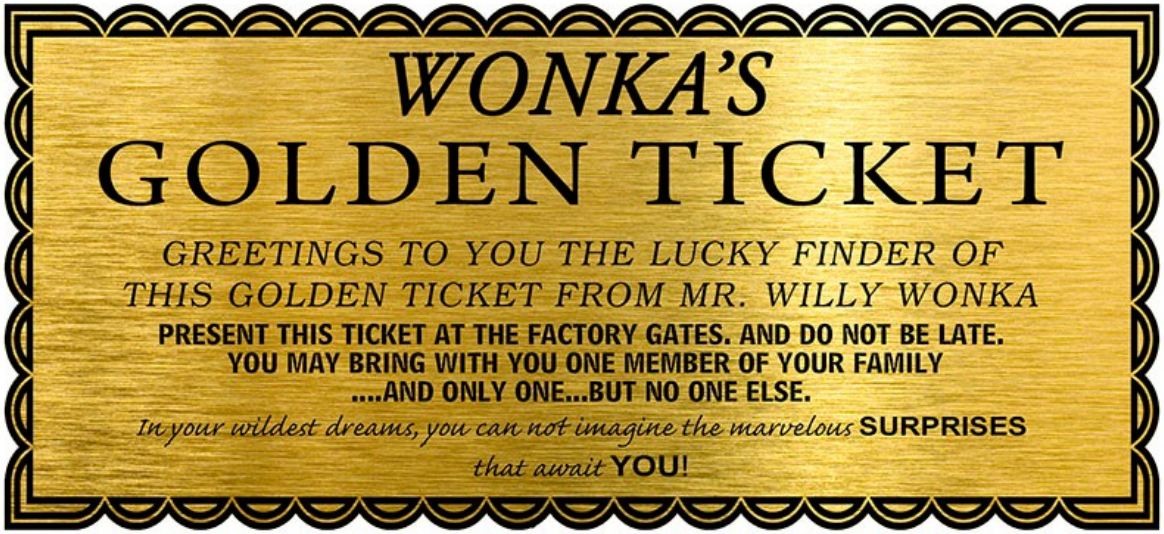
- Ablauf:
  - Angreifer betritt mit gestohlenen Zugangsdaten CITRIX-Server des Unternehmens als lokaler Administrator.
  - Download und Ausführen einer modifizierten Version von Mimikatz.
    - Erster Angriff wohl nicht erfolgreich – keine interessanten Hashes im RAM?!
    - Angreifer stoppte einen Dienst, ein Domain-Admin (!) loggte sich via RDP ein, um das Problem zu untersuchen.
    - Angriff via Mimkatz wurde wiederholt, Hash des Domain-Admins wurde ausgelesen.
  - Offline: Brute-Force-Angriff gegen ausgelesenen NTLM-Hash.
    - Passwort wurde nach wenigen Tagen ermittelt: „`(MaT1=Mu)`“ – 9 Zeichen, komplex!
- Ursachen:
  - Passwörter waren für das Einloggen auf den CITRIX-Server ausreichend.
    Keine 2-Faktor-Authentifizierung vorhanden.
  - Mitarbeiter war als Entwickler lokaler Admin auf dem CITRIX-Server.
  - Anti-Virus hat Schadsoftware nicht erkannt.
    Grund? Obfuscation is easy. :-)
  - Domain-Admin war nicht in der AD-Gruppe „Proteced Users“
    (verfügbar ab Active Directory 2012 R2 Functional Level,
    siehe https://technet.microsoft.com/en-us/library/dn466518.aspx).
  - Administratoren führten alltägliche administrative Arbeiten als Domain-Admin durch.

3. AKT:
ATTACKE GEGEN DIE GESAMTE DOMAIN
(LATERAL MOVEMENT)

VORGEHENSWEISE

- Übernahme weiterer Systeme im Zielnetz via Passwort-Raten oder durch das Nutzen von erbeuteten Passwörtern/Hashes.
  - Zugriff auf Windows-Shares
  - Einloggen via RDP
  - Entfernte Befehlsausführung (Remote Windows Commands)
    - PSExec
    - WMI (Windows Management Infrastructure)
    - ControlUp (https://www.controlup.com/products/controlup)
- Selten: Attacken via Exploits
  - Grund: Wenig Know-How bei den Angreifern.
  - Grund: Wieso schwer, wenn es auch einfach geht?
- Das Ziel der Angreifer
  - Infizieren zentraler Systeme (AD-Controller)
  - Dort: höchste Rechte erhalten.

KERNBOHRUNG FÜR MS ACTIVE-DIRECTORY



- Nähere Informationen:
  - https://www.andreafortuna.org/2020/05/05/(...)
  - https://www.blackhat.com/docs/us-14/(...)

PRAXIS: FALL 2020-01 – GOLDEN TICKET

- Ablauf:
  - Angreifer betreten als Domain Admin den AD-Server.
  - Download und Ausführen einer modifizierten Version von Mimikatz.
  - Auslesen des NTLM-Hashes des Accounts „krbtgt“.
    - Details siehe https://blog.3or.de/mimikatz-deep-dive-on-lsadumplsa-patch-and-inject.html
- Ursachen:
  - Das Netzwerk des Unternehmens war nicht segmentiert.
  - Es wurde mit einem AD für alle Bereiche des Unternehmens gearbeitet.

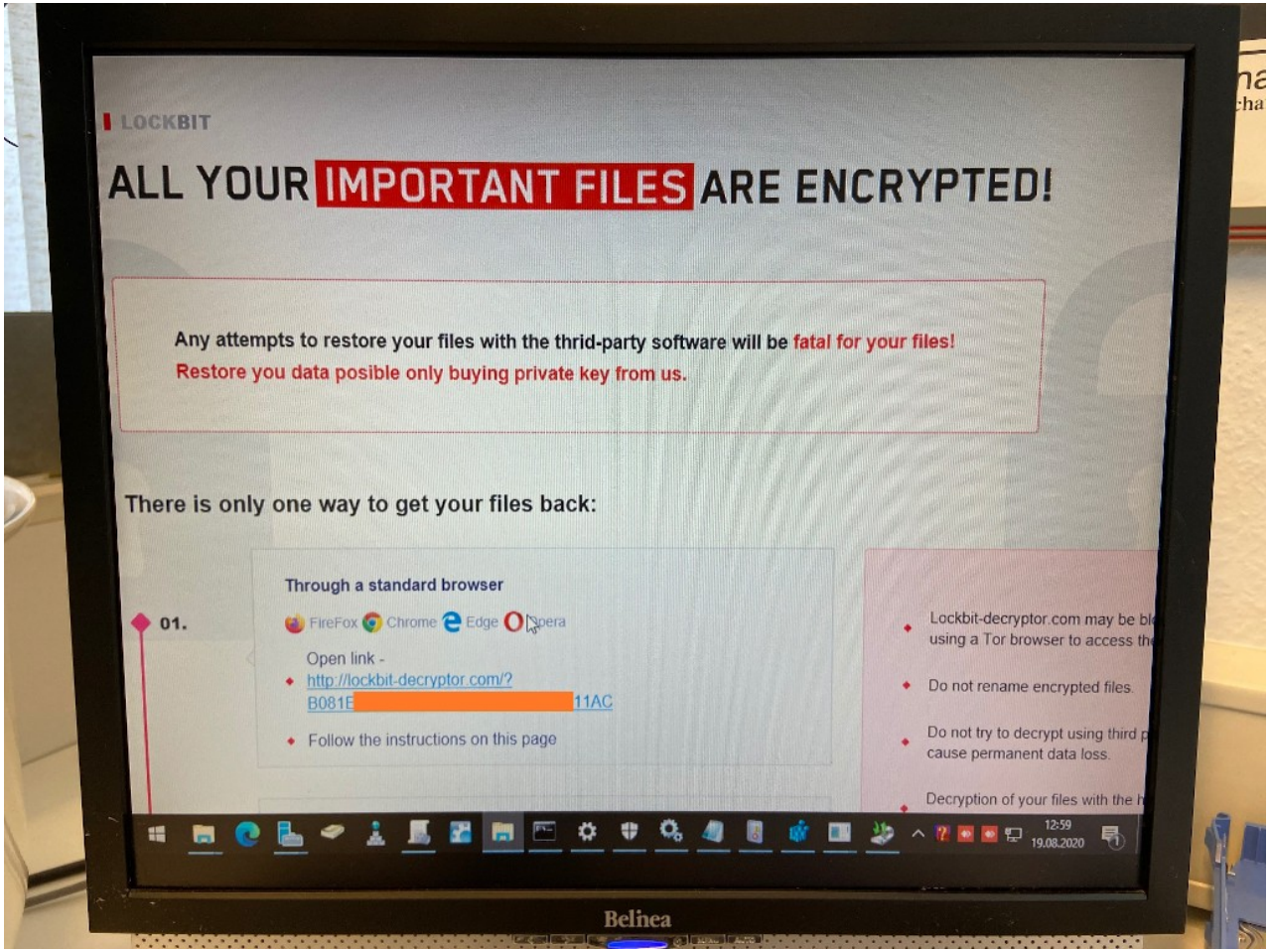
4. AKT: ANGREIFER HAT FREIES SPIEL

(DIE WELLE BAUT SICH AUF)

PRAXIS: FALL 2021-04 – KOMPLETTE ÜBERNAHME

- Ablauf:
  - Endpoint-Security (Sophos) domainweit abgeschaltet.
  - Logging wurde vom Angreifer ignoriert.
  - Einsatz eines Scripts zum Auslesen der in den Browsern gespeicherten Passwörter auf den zentralen Fileservern.
  - Kopie der Datenbanken der zentralen ERP- und CRM-Applikation.
  - Sabotieren der Datensicherung.
    - Login auf einem Backup-Filer.
    - Löschen des gesamten Filers (inkl. Sektor-Optimierung).
    - Löschen sämtlicher Backup-Jobs.
  - Ausrollen der Verschlüsselungssoftware via Group-Policy.
- Ursachen (Auswahl):
  - Backup-Filer war im AD eingebunden.
  - Backup-Filer war aus dem Produktivnetz erreichbar.

PRAXIS: FALL 2020-14 – VERSCHLÜSSELT



PRAXIS: FALL 2021-04 - SCHÄDEN

- Lösegeld
  - 1,6 Mio € (ursprünglich gefordert: 4,2 Mio €)
- Sonstige Kosten
  - ca. 11-13 Mio €

WIE KANN MAN SICH EFFEKTIV SCHÜTZEN?

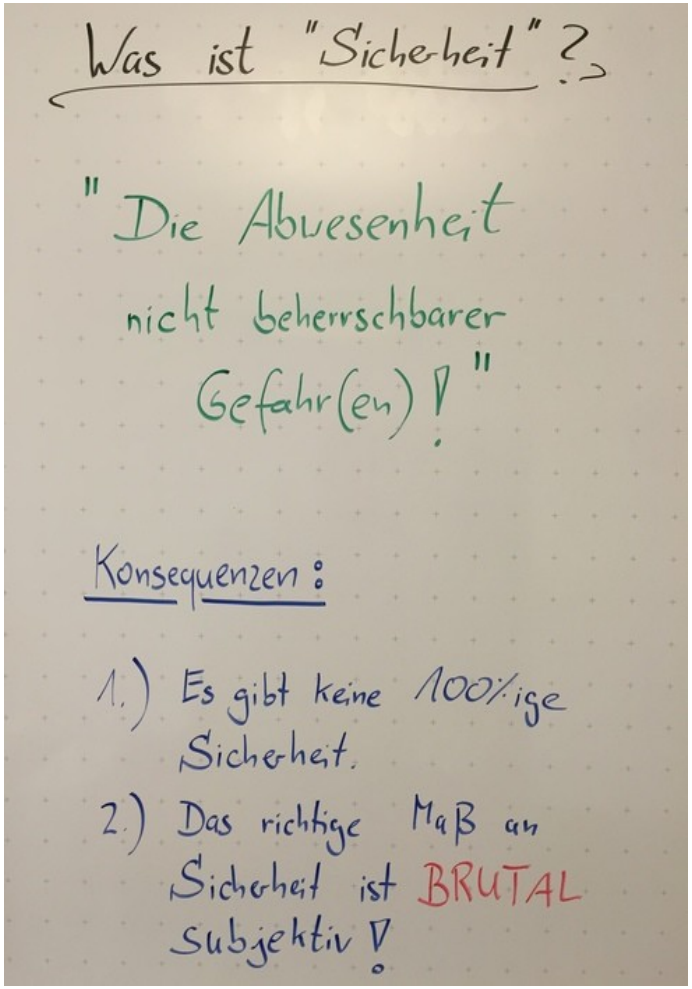
INTERMEZZO

(DIE ZIELE DER INFORMATIONSSICHERHEIT)

-

AUSZUG AUS DEN BEREICH „GRUNDLAGEN“ MEINES 2-TAGES-SEMINARS ZUR VDS 10000

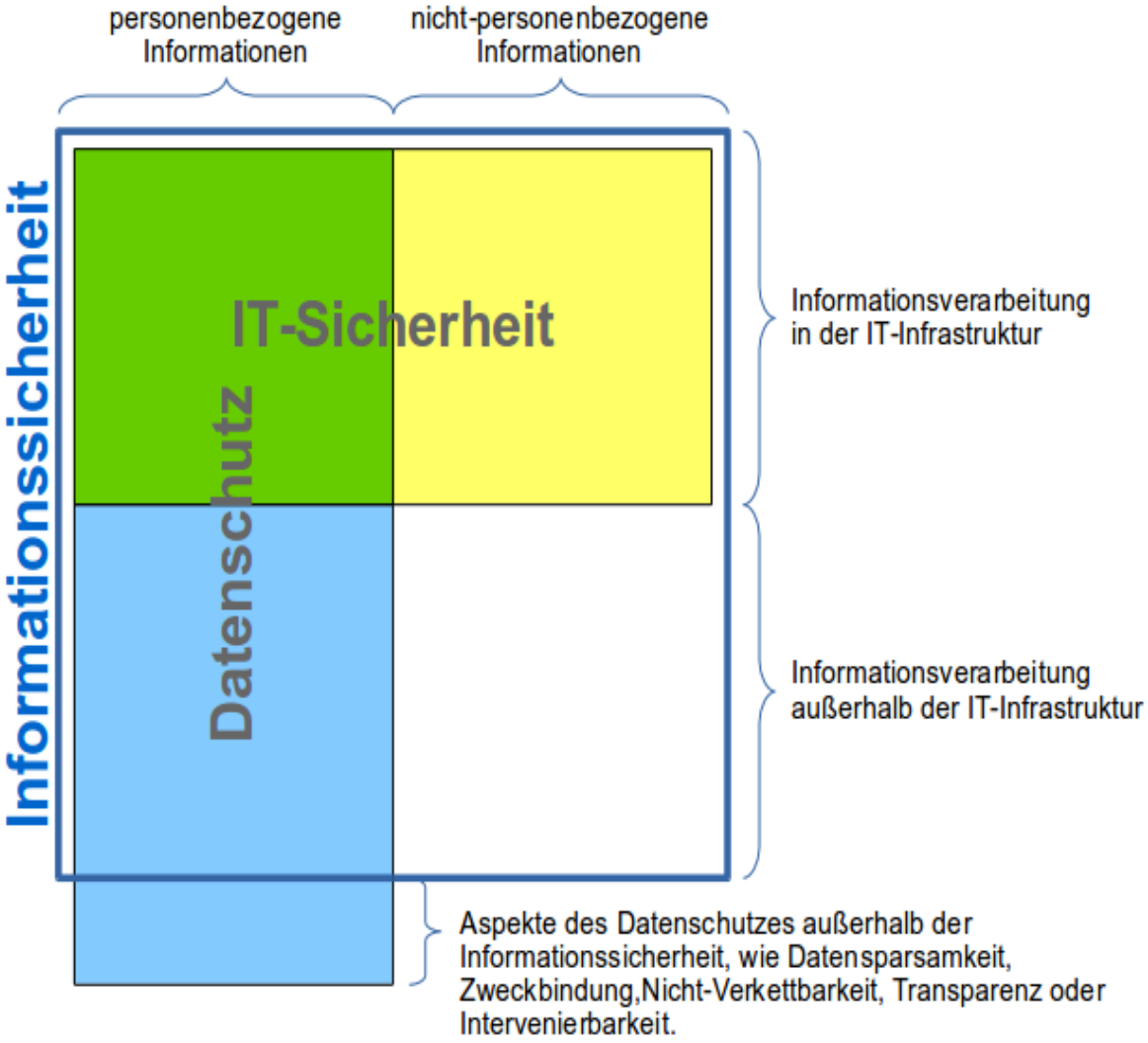
Begriffsdefinition: Sicherheit



Die nebenstehende Definition impliziert:

- Wenn Sie sich um (Informations-)Sicherheit kümmern wollen/sollen/müssen, arbeiten Sie vor allem mit Menschen.
- Informationssicherheit ist keine Frage der technischen Ausstattung, sondern ein Teamsport in verschiedenen Disziplinen.
- Diplomatie ist gefragt!
  Sie müssen zuhören, argumentieren, akzeptieren, Kompromisse eingehen.
- Sie sind Techniker, Sozialpädagoge und Außenminister in einer Person.

Informationssicherheit, IT-Sicherheit, Datenschutz



- Informationssicherheit:
  Sicherstellen der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen.
- IT-Sicherheit:
  Schutz der elektronischen Informationsverarbeitung. Untermenge der Informationssicherheit.
- Datenschutz:
  Der Schutz des Einzelnen vor Missbrauch seiner personenbezogenen Informationen.

INTERMEZZO
ENDE

SCHUTZ FÜR KLEIN- UND KLEINSTUNTERNEHMEN

ZWICKMÜHLE UND LÖSUNG

- Klein- und Kleinstunternehmen sowie vergleichbare Organisationen haben in aller Regel wenige Ressourcen für die Sicherheit ihrer IT.
- Es fehlen im Alltag die finanziellen Mittel, freie Arbeitszeit und entsprechendes Wissen.
- Klein- und Kleinstunternehmen müssen aber nicht zu Fort Knox werden. Das notwendige Sicherheitsniveau kann erreicht werden, indem einige wenige Maßnahmen gezielt und mit Augenmaß umgesetzt werden.
- Diese Maßnahmen…
  - …sind wohl bekannt
  - …können kostengünstig implementiert werden und
  - …haben sich seit Jahren nicht geändert (sie sind statisch).

DIE WICHTIGSTEN MAßNAHMEN

- Arbeitsabläufe festlegen
  - Klare Regelungen für Mitarbeiter: Was ist erlaubt, was untersagt?
  - Wie werden IT-Systeme in Dienst genommen und ausgemustert?
  - Was geschieht bei einem Wechsel der Tätigkeit oder bei Ausscheiden eines Mitarbeiters?
- Härten der IT-Systeme
  - Anti-Virus
  - Updates
  - Authentifizierung
- Datensicherung
  - Stellen Sie fest, wo die Unternehmensdaten gespeichert sein.
  - Sorgen Sie dafür, dass diese Speicherorte in angemessenen Abständen (i. d. R. täglich) gesichert werden.
  - Schotten Sie Ihre Backup-Systeme vom Rest Ihrer IT so weit wie möglich ab.
  - Entwickeln Sie für jeden Speicherort einen Wiederanlaufplan.
  - Testen Sie Datensicherungen und Wiederanlaufpläne.

SCHUTZ BEI HÖHEREN SICHERHEITS-ANFORDERUNGEN

WAS IST NOTWENDIG?

- Wenn Organisationen in einem verstärken Maße auf ihre Informationsverarbeitung angewiesen sind oder sie über eine komplexere IT-Infrastruktur verfügen wird ein maßgeschneidertes Sicherheitskonzept benötigt, das sich an neue technische, organisatorische, rechtliche und vertragliche Herausforderungen anpasst.
- Ein solches System wird Informationssicherheitsmanagementsystem (ISMS) genannt.

WAS IST EIN ISMS?

- Ein Informationssicherheitsmanagementsystem (ISMS)…
  - …ist eine Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern (anzupassen).
  - …stellt sicher, dass Informationssicherheit nach dem Motto „So viel wie nötig, so wenig wie möglich“ implementiert und auf dem aktuellen Stand gehalten wird.
  - …ist quasi Qualitätsmanagement für die Informationssicherheit.

WAS IST EIN ISMS?

- In der Praxis lassen sich die Eigenschaften und Ziele eines ISMS wie folgt definieren (1):
  - Verankerung in der Organisation:
    Die Verantwortlichkeiten und Befugnisse für den Informationssicherheitsprozess werden vom Topmanagement eindeutig und widerspruchsfrei zugewiesen. Insbesondere wird ein Mitarbeiter bestimmt, der umfassend verantwortlich für das Informationssicherheitsmanagementsystem ist (in der Regel Informationssicherheitsbeauftragter oder kurz ISB).
  - Verbindliche Ziele:
    Die durch den Informationssicherheitsprozess zu erreichenden Ziele werden durch das Topmanagement vorgegeben.
  - Richtlinien:
    Verabschiedung von Sicherheitsrichtlinien (Security Policies), die den sicheren Umgang mit der IT-Infrastruktur und den Informationen definieren.
  - Personalmanagement:
    Bei Einstellung, Einarbeitung sowie Beendigung oder Wechsel der Anstellung von Mitarbeitern werden die Anforderungen der Informationssicherheit berücksichtigt.

WAS IST EIN ISMS?

- In der Praxis lassen sich die Eigenschaften und Ziele eines ISMS wie folgt definieren (2):
  - Aktualität des Wissens:

    Es wird sichergestellt, dass die Organisation über aktuelles Wissen in Bezug auf Informationssicherheit verfügt.
  - Qualifikation und Fortbildung:

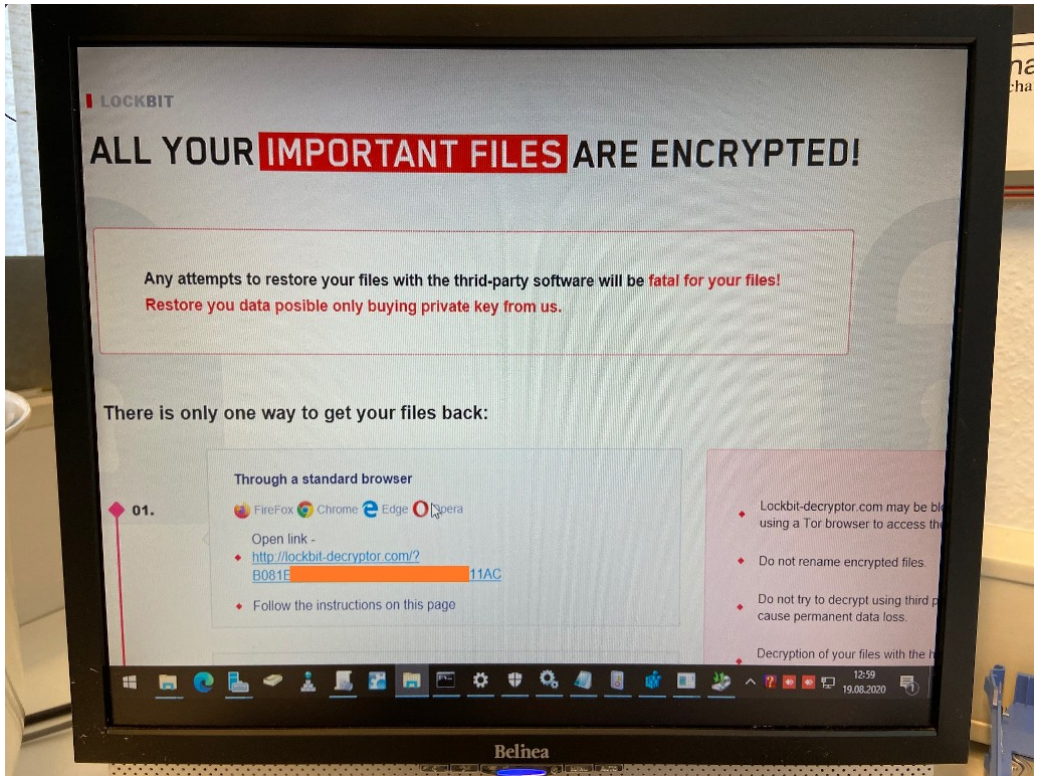
    Es wird sichergestellt, dass das Personal seine Verantwortlichkeiten versteht und es für seine Aufgaben geeignet und qualifiziert ist.
  - Adaptive Sicherheit:

    Das angestrebte Niveau der Informationssicherheit wird definiert, umgesetzt und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage angepasst (Kontinuierlicher Verbesserungsprozess).

KONKRETES VERHALTEN BEI RANSOMWARE-ATTACKEN

WENN ES BEREITS ZU SPÄT IST… (1)

» Das ist die häufigste Situation:



WENN ES BEREITS ZU SPÄT IST… (2)

- Start der Dokumentation
  - Tagebuch!
- Überblick gewinnen
  - Welche Teile der IT-Infrastruktur sind betroffen?
  - Dokumentation starten.
- Leib und Leben von Personen schützen
  - Entsprechende Vorgehensweisen abarbeiten.
- Sofort-Maßnahmen (am besten parallel abarbeiten: Team!)
  - Alle IT-Systeme offline nehmen (geordnet herunterfahren bzw. einfrieren).
  - Datensicherungen offline nehmen.
  - Topmanagement benachrichtigen.
  - Versicherung involvieren (falls vorhanden).
  - Team bilden, ggf. externe Unterstützung einholen.
  - Sind ggf. weitere Organisationen betroffen? Benachrichtigen!

WENN ES BEREITS ZU SPÄT IST… (3)

- Schaden dokumentieren
  - Bestandsaufnahme: Welche Systeme sind verschlüsselt?
- Beweismittel sichern
  - Rücksprache mit Versicherungen und/oder Strafverfolgungsbehörden.
- Schaden beheben
  - Die gesamten verschlüsselten IT-Systeme werden gesichert.
    - Beweismittel (siehe oben).
    - Für den Fall, dass das Entschlüsseln bzw. Zurückspielen nicht funktionieren sollte.
  - Kein Backup?
    - Mit den Erpressern verhandeln
    - Geld zahlen, Schlüssel erhalten und Daten entschlüsseln.
  - Backup vorhanden? Wiederherstellung der gesamten betroffenen IT, dabei begleitend
    - Analyse und Entfernen der Verschlüsselungssoftware.
    - Golden Ticket entsorgen.
      (2x Passwort von Account „krbtgt“ auf AD-Controller zurücksetzen)
    - Suche und Entfernen von Backdoors.
- Nachbereitung
  - IT-Infrastruktur engmaschig überwachen.
  - Strukturierte Ursachensuche.
  - Implementieren der gelernten Verteidigungsmechanismen.
  - ISMS aufbauen!

WENN GERADE VERSCHLÜSSELT WIRD… (1)

- Situation:
  Einige wenige IT-Systeme sind verschlüsselt, aber ansonsten scheint alles normal zu sein.
- Überblick gewinnen?
  - Unnötig. Es ist Gefahr im Verzug. Handeln!
- Leib und Leben von Personen schützen
  - Klären: Welche IT-Systeme dürfen absolut NICHT abgeschaltet werden?
- Sofort-Maßnahmen (am besten parallel abarbeiten: Team!)
  - Alle IT-Systeme kalt ausschalten (Notaus!).
  - IT-Systeme die nicht abgeschaltet werden dürfen werden contained.
  - Datensicherungen offline nehmen.
  - Topmanagement benachrichtigen.
  - Team bilden, ggf. externe Unterstützung einholen

WENN GERADE VERSCHLÜSSELT WIRD… (2)

- Schaden dokumentieren
  - Welche Teile der IT-Infrastruktur sind betroffen?
  - Bestandsaufnahme: Welche Systeme sind verschlüsselt?
- Beweismittel sichern
  - Rücksprache mit Versicherungen und/oder Strafverfolgungsbehörden.
- Schaden beheben
  - Jedes IT-System behandeln.
    - Booten von CD bzw. USB-Stick.
    - Wenn verschlüsselte Dateien anwesend sind: System für Wiederherstellung vormerken; weiter zum nächsten System.
    - Suchen und Entfernen der Verschlüsselungssoftware.
    - AD-Controller: Golden Ticket entsorgen. (2x Passwort von Account „krbtgt“ auf AD-Controller zurücksetzen)
    - Suchen und Entfernen von Backdoors.
    - Logging etablieren.
- Nachbereitung
  - IT-Infrastruktur engmaschig überwachen.
  - Strukturierte Ursachensuche.
  - Implementieren der gelernten Verteidigungsmechanismen.
  - ISMS aufbauen!

IT-DIENSTLEISTER WURDE VERSCHLÜSSELT? (1)

- Situation:
  Der IT-Dienstleister wurde verschlüsselt (bzw. hat Eindringlinge entdeckt). Er hat sich gemeldet und sie gewarnt.
- Überblick gewinnen
  - Informationen vom Dienstleister einfordern.
    - Welche Attacken wurden durchgeführt?
    - Wie hat er sie erkannt?
  - Auf welche IT-Systeme hatte der Dienstleister Zugriff?
  - Welche Berechtigungen hatte der Dienstleister?
- Leib und Leben von Personen schützen
  - Klären:
    - Welche IT-Systeme müssen absolut verfügbar sein?
    - Welche Informationen müssen absolut vertraulich sein?
- Sofort-Maßnahmen (am besten parallel abarbeiten: Team!)
  - Datensicherung prüfen!
  - Datensicherungen offline nehmen.
  - Internetverbindung kappen.
  - Team bilden, ggf. externe Unterstützung einholen

IT-DIENSTLEISTER WURDE VERSCHLÜSSELT? (2)

- Schaden dokumentieren
  - Kommunikation mit dem IT-Dienstleister speziell sichern.
- Beweismittel sichern
  - siehe oben
- Schaden beheben
  - Nach bekannten Angriffsmustern suchen.
    - AD-Controller: Golden Ticket entsorgen.
      (2x Passwort von Account „krbtgt“ auf AD-Controller zurücksetzen)
    - Suchen und Entfernen von Backdoors.
    - Logging etablieren.
- Nachbereitung
  - Strukturierte Ursachensuche.
  - Implementieren der gelernten Verteidigungsmechanismen.
  - ISMS aufbauen!

KONTAKTDATEN

MEINE KONTAKTDATEN

- Telefon: +49 163 732 74 75
- Mail: sicherheit [at] mark [minus] semmler [dot] de
- IM: Threema (ID: VTH4PXRW), Signal, Wire, Telegram
- Web: https://www.mark-semmler.de

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT