IT-Sicherheit Rückblick 2020

@cmitasch
Christoph Mitasch, Thomas-Krenn.AG

Webinar, 21. Jänner 2021

THOMAS KRENN®

Über mich

- Christoph Mitasch
- seit 2005 bei der Thomas-Krenn.AG Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner (v1)

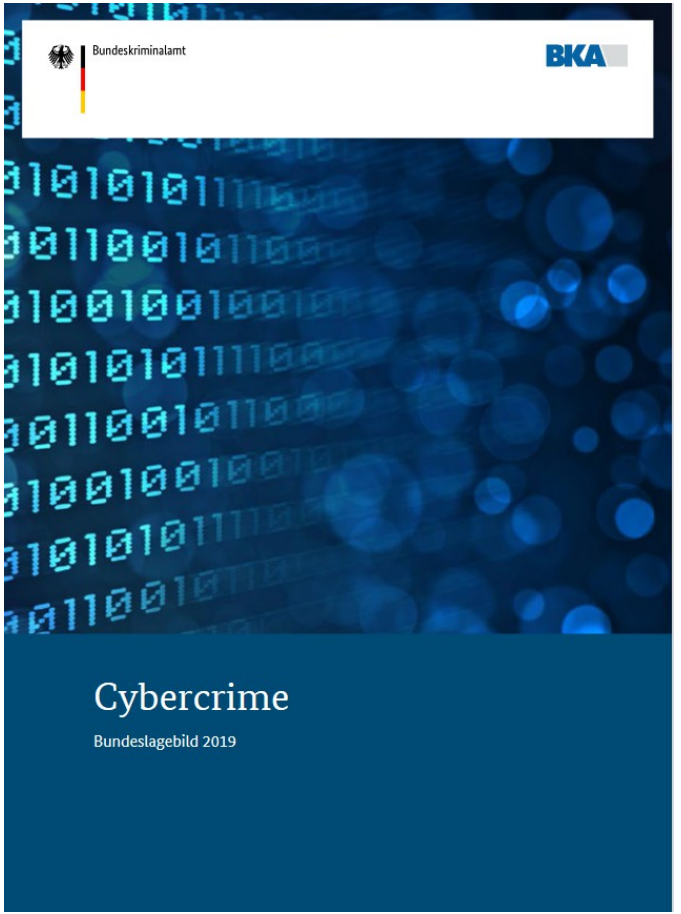
Agenda

- Lagebericht BSI und BKA
- Hardware-Lücken
- Solarwinds-Hack
- IT-Sicherheitsgesetz 2.0

Agenda

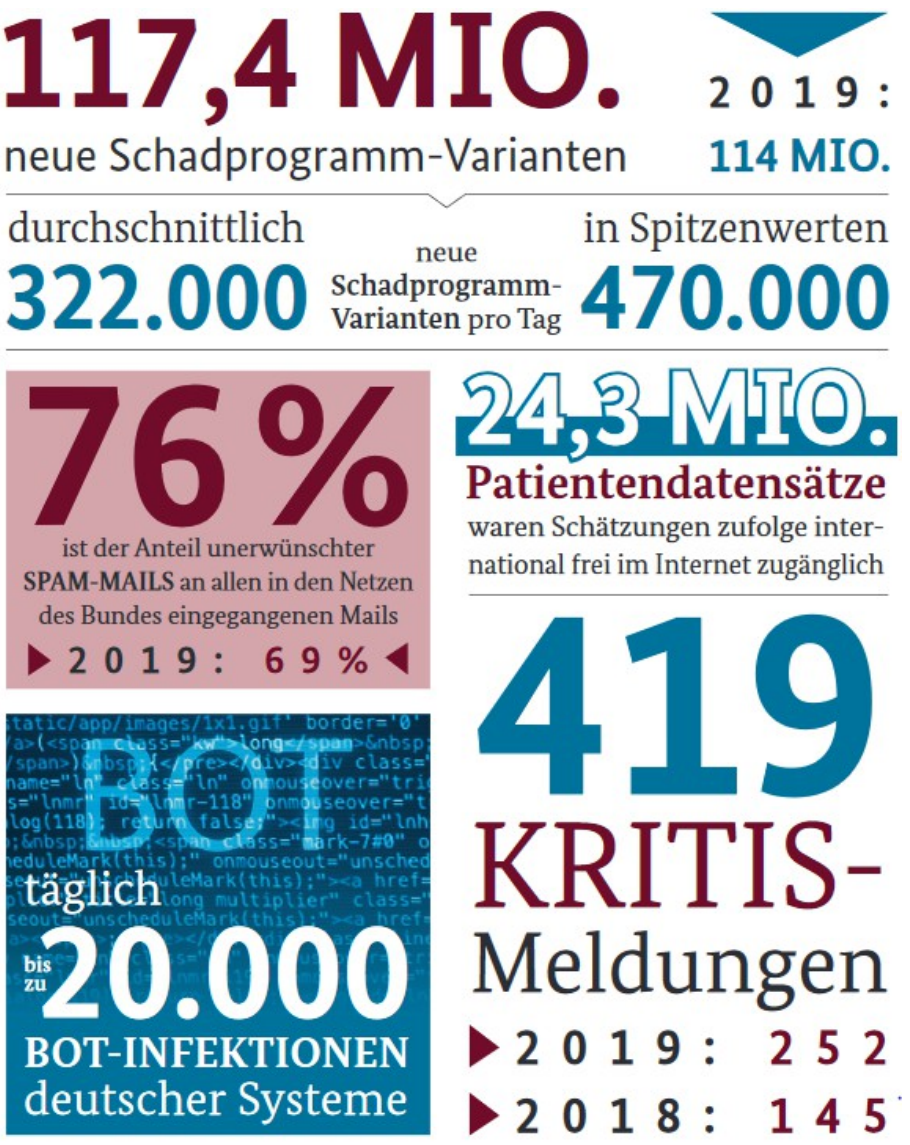
- Lagebericht BSI und BKA
- Hardware-Lücken
- Solarwinds-Hack
- IT-Sicherheitsgesetz 2.0

Lagebericht BSI und BKA



Lagebericht BSI

- Schadsoftware
  - Emotet – Trickbot - Ryuk
    - auch passwortgeschützte Archive
    - deutsche Anhänge
    - Trickbot → Trickboot
  - Ransomware
  - → Backup essentiell
- Datenleck
  - z.b. Autovermieter mit 9 Millionen Mietverträgen bis 2003
  - kleine Fehler, große Auswirkungen

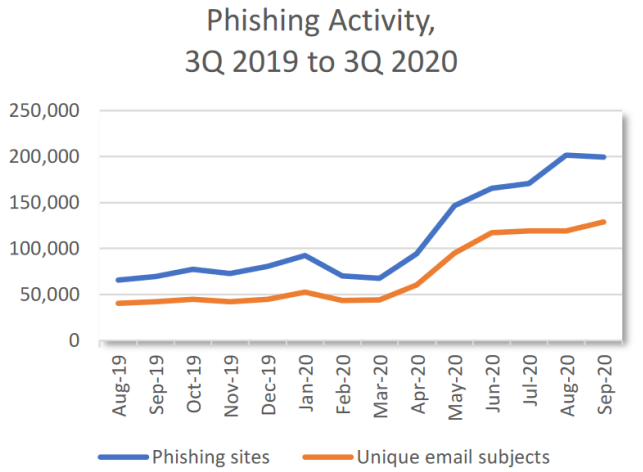


Lagebericht BSI

- Software
  - EOL Windows 7 und Server 2008
  - EOL Flash Player
  - Citrix-Lücken #Shitrix
    - Uni Düsseldorf mit Todesfall
    - Update reicht nicht immer aus
      Backdoor könnte schon davor eingerichtet worden sein
- APT und DDOS
  - Qualifizierte Dienstleister vom BSI gegen APT und DDOS
  - https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/Qualifizierte_Dienstleister/QDL_node.html

Lagebericht BSI

- Phishing
  - Links mehrheitlich HTTPS
  - Anstieg im 2.HJ
- Covid-19
  - Social Engineering
  - Ad hoc Home-Office
  - Digitalisierungsschub
    → mehr Angriffsfläche
  - Bsp: Soforthilfe



Quelle: https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf

COVID-19 Soforthilfe-Maßnahmen durch Cyber-Kriminelle missbraucht

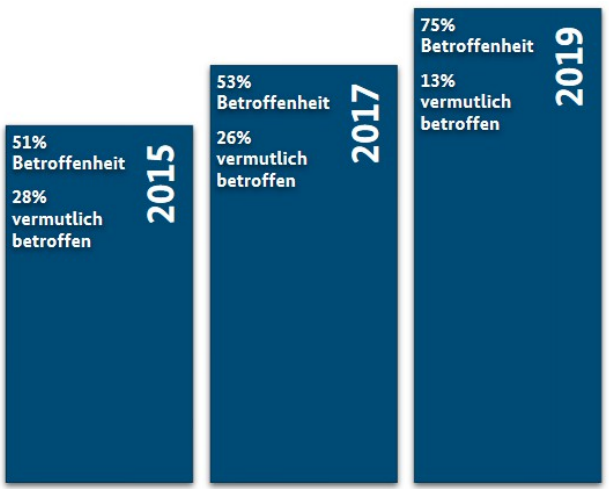
Sachverhalt

Nahezu unmittelbar nach Bekanntgabe und Umsetzung der finanziellen Soforthilfe-Maßnahmen auf Bundes- und Länderebene Ende März 2020 wurden *Phishing*-Kampagnen beobachtet, die versuchten, diese Maßnahmen auszunutzen. Betrüger registrierten dafür *Phishing*-Domains und gestalteten die darunter erreichbaren Webseiten teilweise identisch zu den offiziellen Soforthilfe-Seiten. Anschließend wurden diese Seiten mit unterschiedlichen Mitteln wie *Spam*-E-Mails oder Platzierungen in Suchmaschinen in Umlauf gebracht. Es ist davon auszugehen, dass das grundlegende Ziel dieser *Phishing*-Versuche die Sammlung von Informationen über finanziell notleidende Unternehmen und Privatpersonen war. Diese Informationen konnten die Angreifer anschließend verwenden, um bei den offiziellen Soforthilfe-Stellen Zahlungen im Namen der Opfer abzurufen, wodurch dem eigentlich berechtigten Antragssteller etwaige Hilfeleistungen zumindest vorübergehend verwehrt wurden und dem Staat erheblicher Schaden entstanden ist. Langfristig ist auch die Verwendung der durch das *Phishing* gewonnen Informationen für Folgeangriffe auf die Opfer nicht auszuschließen.

Quelle: BSI Lagebericht 2020

Cybercrime Bundeslagebild BKA

_ bekannt gewordenen Straftaten



Drei von vier Unternehmen wurden 2019 Opfer von Cyberkriminellen – 2017 nur jedes zweite.

100.514 Fälle von Cybercrime im engeren Sinne (+15,4%)

294.665 Fälle, bei denen das Internet als Tatmittel genutzt wurde (+8,4%)

78.201 Fälle von Computerbetrug (+18,0%)

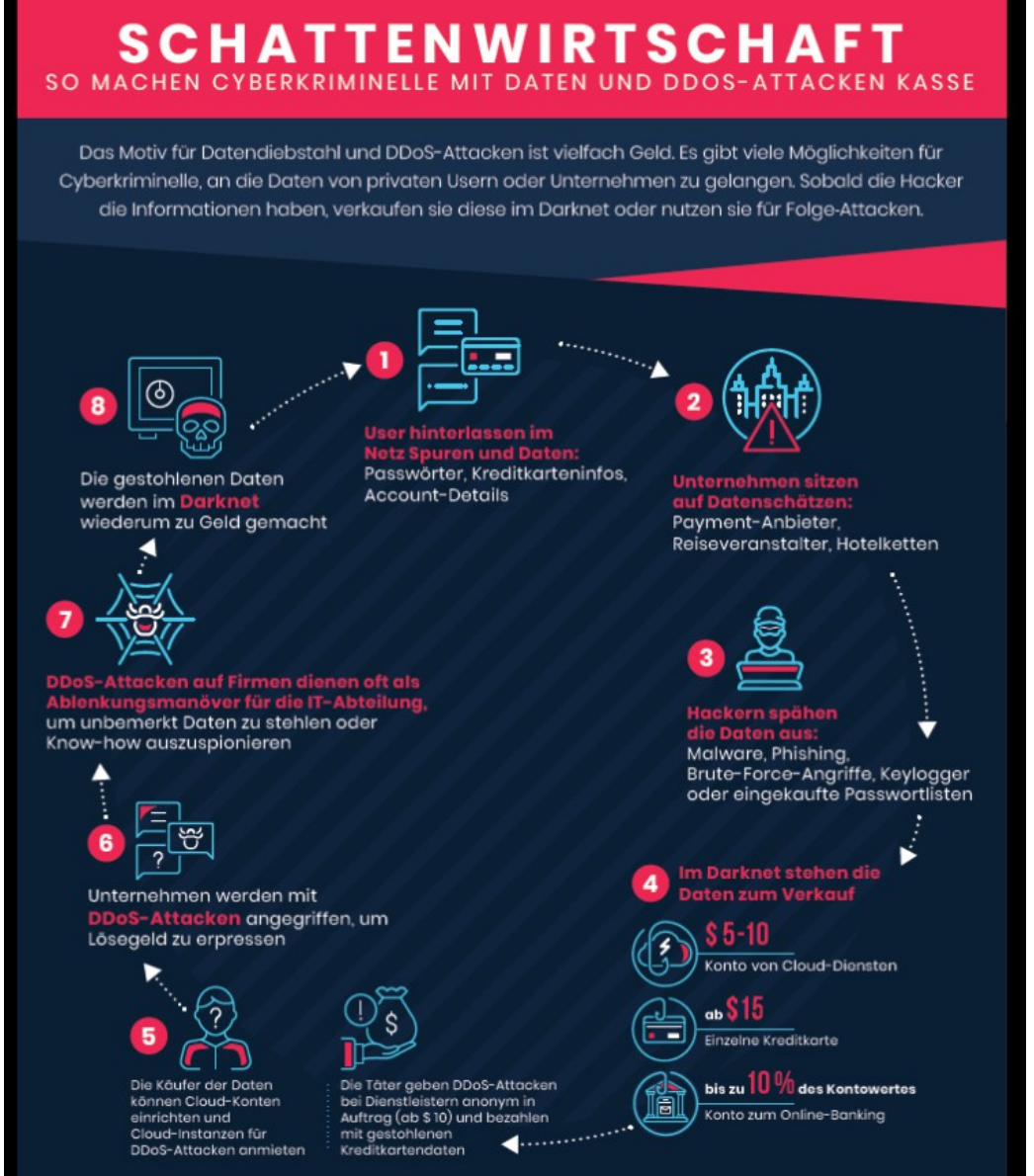
87,7 Mio. Euro Schaden im Bereich Computerbetrug (+44,4%)

9.926 Fälle von Ausspähen/Abfangen von Daten (+13,3%)

8.877 Fälle von Fälschung beweiserheblicher Daten/Täuschung im Rechtsverkehr (+5,1%)

3.183 Fälle von Datenveränderung/ Computersabotage (+10,7%)

Quelle: BKA Bundeslagebild 2019



Quelle: Bundeslagebild BKA / Link 11

Diebstahl digitaler Identitäten

- Handelsware der Underground Economy
- Jede gestohlene digitale Identität ist Nährboden für weitere kriminelle Aktivitäten.

Malware

- *Emotet* bleibt größte Malware-Bedrohung – v. a. im Verbund mit *TrickBot* und *Ryuk*
- Anzahl der Malware-Familien steigt stetig an
- Professionelles Crypting, das die Malware gegenüber AV-Scannern unsichtbar werden lässt

Ransomware

- Die primäre, existentielle Bedrohung für Unternehmen
- Systeme werden nicht mehr nur verschlüsselt – Akteure drohen mit der Veröffentlichung der kryptierten Daten.

DDoS

- Sowohl Quantität als auch Qualität steigend
- Vermehrter Nutzen von IoT und Clouds zur Verstärkung von DDoS-Angriffen

Underground Economy

- Arbeitsteilige, hochspezialisierte Wirtschaft
- Basiert auf neun Säulen – jede mit ihrem eigenen Fachgebiet
- Jede Säule sorgt für den reibungslosen Ablauf von kriminellen Aktivitäten.

Angriffe auf Unternehmen

- APT-ähnliches Verhalten durch kriminelle Organisationen
- Schaden durch z. B. einen Ransomware-Angriff liegt im mind. 6-stelligen Bereich

Entwickeln Sie ein angemessenes IT-Sicherheitskonzept für Ihr Unternehmen

- Entwerfen Sie Verfahrensweisen und Anleitungen, wie sich Ihre Mitarbeitenden im Falle eines Cyberangriffs verhalten sollen.
- Aktualisieren Sie Ihr Sicherheitskonzept regelmäßig.
- Schulen Sie Ihre Mitarbeitenden hinsichtlich Cybersicherheit.
- Legen Sie (vom System getrennte) Back-Ups Ihres Systems an.

Wie Sie helfen können

- Seien Sie zurückhaltend bei der Weitergabe von vertraulichen und persönlichen Informationen.
- Haben Sie gesundes Misstrauen, wenn Ihnen etwas ungewöhnlich vorkommt.
- Überprüfen Sie E-Mails auf die richtige Absenderadresse.
- Öffnen Sie keine verdächtigen E-Mails.
- Seien Sie misstrauisch bei Links oder Anlagen in E-Mails unbekannter Absender.

Maßnahmen nach einer Ransomware-Infektion

- Trennen Sie unverzüglich die Netzwerkverbindung von infizierten Rechnern und schalten Sie betroffene Geräte umgehend aus.
- Isolieren Sie Backups, damit diese nicht ebenfalls verschlüsselt werden.
- Sichern Sie relevante Dateien, die Aufschluss über den Infektionshergang geben können. Hierzu zählen beispielsweise Log-Dateien oder E-Mails.
- Ändern Sie sämtliche Benutzer- und Netzwerkkennwörter, sofern diese durch den Vorfall kompromittiert sein könnten.
- Erstatten Sie unverzüglich Strafanzeige bei Ihrer Zentralen Ansprechstelle Cybercrime (ZAC).

Wenden Sie sich an die Polizei!

- Erstatten Sie auf jeden Fall Anzeige.
- Informieren Sie sich über die ZAC-Dienststellen: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
- Wir appellieren dringend, bei Cyberangriffen jeder Art unverzüglich Strafanzeige zu erstatten – erfolgreiche Cyberkriminelle werden Angriffe wiederholen!

Quelle: BKA Bundeslagebild 2019

Agenda

- Lagebericht BSI und BKA
- Hardware-Lücken
- Solarwinds-Hack
- IT-Sicherheitsgesetz 2.0

WLAN-Lücke „Kr00k“

Quelle: https://www.eset.com/int/kr00k/

- Broadcom und Cypress WLAN-Chips betroffen
- CVE-2019-15126
  - 01/2019 Bericht an Amazon, 02/2020 Disclosure
- ca. 1 Mrd betroffene Geräte
  - Amazon Echo 2nd gen/Kindle 8th gen
  - Apple iPad mini 2/iPhone 6, 6S, 8, XR/MacBook Air Retina 13-inch 2018
  - Google Nexus 5/6/6P
  - Raspberry Pi 3
  - Samsung Galaxy S4 GT-I9505/Galaxy S8
  - Xiaomi Redmi 3S
  - Plus APs: Asus RT-N12, Cisco, Huawei B612S-25d/EchoLife HG8245H/E5577Cs-321

WLAN-Lücke „Kr00k“

Quelle: https://www.eset.com/int/kr00k/

- Variante für Qualcomm und MediaTek (CVE-2020-3702)
  - ASUS RT-AC52U router
  - MediaTek’s MT3620 (Azure Sphere OS)
- Testskript
  - https://github.com/eset/malware-research/tree/master/kr00k
- Funktionsweise:
  - WPA2 mit CCMP
  - Empfangs-Buffer mit genulltem Schlüssel kann ausgelesen werden
  - nur unverschlüsselter WLAN-Traffic (ohne TLS) betroffen

BIOS-Sicherheitsupdates 2020

LGA 1151-2 - 8th Gen

- Prozessoren: Coffee Lake (8th Generation Intel Core Processor Family) / Coffee Lake Refresh (9th Generation Inte
- SPS Version: 05.00.* und 05.01.*

Sicherheitsupdate	2020.2 IPU INTEL-SA-00381 INTEL-SA-00389 INTEL-SA-00391	2020-09-08 INTEL-SA-00347 INTEL-SA-00356 INTEL-SA-00404	2020.1 IPU INTEL-SA-00295 INTEL-SA-00320 INTEL-SA-00322	2020-01 INTEL-SA-00329	2019-12 INTEL-SA-00289 INTEL-SA-00317	2019.2 IPU INTEL-SA-00220 INTEL-SA-00241 INTEL-SA-00254 INTEL-SA-00270
Update Microcode	ja	in Abklärung	ja	ja	ja	ja
Update SPS	ja	in Abklärung	ja	-	-	ja
Update Platform Sample / Silicon Reference firmware	in Abklärung	in Abklärung	in Abklärung	-	-	ja
Update BIOS ACM Firmware / SINIT ACM Firmware	in Abklärung	in Abklärung	in Abklärung	-	-	ja
ASUS P11C-I	betroffen, Microcode und ME Firmware Update erforderlich	in Abklärung	BIOS 3301			

https://www.thomas-krenn.com/de/wiki/BIOS_Sicherheitsupdates

Intel Platform Update (IPU)

- 2-3x pro Jahr
- 06/2020: **IPU 2020.1**
  - 5 Advisories, 25 Vulnerabilities
  - CVE-2020-0594 und CVE-2020-0595 mit CVSS-Score: 9,8 betrifft AMT und IPv6
  - CVE-2020-0543 „Crosstalk“ über mehrere CPU-Kerne hinweg, bei VM-Betrieb relevant
- 11/2020: **IPU 2020.2**
  - 40 Advisories, 95 Vulnerabilities
  - CVE-2020-12321 mit CVSS-Score: 9,6 Bluetooth
  - CVE-2020-8752 mit CVSS-Score 9,4 betrifft AMT und IPv6

Magnetkarten im Jahr 2020…

Heute.at

68 Schließfächer geknackt: Schaden über 20 Millionen €

Zusammen mit den Daten aus den Magnetkarten hatten die Täter alle ...
Mit den gestohlenen Codes holten sie ein Schließfach nach dem ...

vor 1 Monat

Quelle: Google News

- November 2020
- Magnetkarten mit Skimming kopiert
  → „Stand der Technik“ trifft vmtl. nicht zu
- Zutrittscodes mit Mini-Kamera erspäht

Entschädigung für Kunden denkbar

Den "Salzburger Nachrichten" zufolge besteht für die betroffenen Bankkunden nun Hoffnung auf Entschädigung. Die Geldinstitute sollen bereits freiwillige Zahlungen zugesagt haben. Im Gegenzug sei die Zustimmung zu einer Geheimhaltungsvereinbarung verlangt worden.

Quelle: https://www.salzburg24.at/news/oesterreich/bankschliessfach-coup-in-wien-neue-details-98083483

Agenda

- Lagebericht BSI und BKA
- Hardware-Lücken
- Solarwinds-Hack
- IT-Sicherheitsgesetz 2.0

Solarwinds-Hack

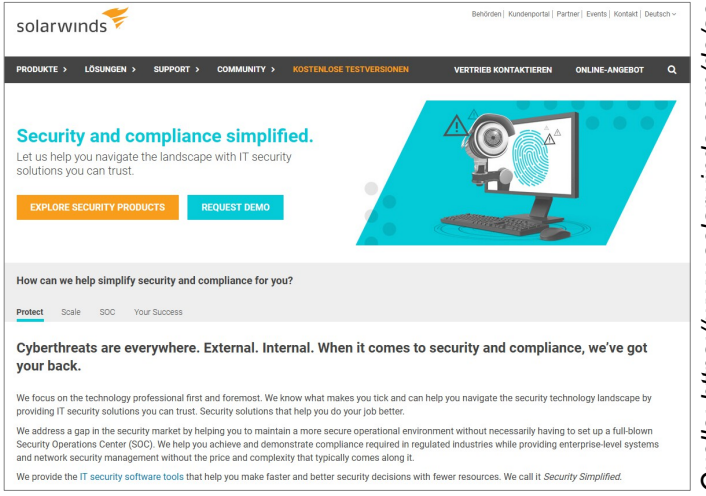
- Schadsoftware Sunburst (MS: Solorigate)
  via Update für Software Orion an ca. 18.000 Kunden verteilt
- Update März 2020, Dezember 2020 wurde Angriff bekannt
- Command & Control Server in Orion integriert
  (u.a. Dateien kopieren und ausführen, Reboot, Dienste steuern)
- Betroffene u.a. FireEye, VMware, Microsoft,
  Finanz-/Landwirtschafts-/Handelsministerium der USA, National Nuclear Security Administration, Homeland Security, ...
- Office-365-Mailboxen bei US-Justizministerium zugreifbar
- bei Micosoft war Quellcode einsehbar

Solarwinds-Hack

- Sunburst in gültig signierter DLL enthalten
- Netzwerk Traffic über Orion Improvement Program (OIP) Protokoll getarnt, Ergebnisse in Orion Plugin Konfigurationsdateien
- Orion-Update installieren reicht nicht aus
  → forensische Analyse und Neuinstallation notwendig
- Supernova ist ein zweites Backdoor, vermutlich kein Zusammenhang mit Sunburst, derzeit keine Angriffe darüber bekannt

> How did you detect the intrusion?
>
> The intrusion was detected by monitoring secondary registrations of our Two-Factor authentication and reporting on suspicious behavior.

Quelle: https://www.fireeye.com/current-threats/sunburst-malware.html



Quelle: https://www.solarwinds.com/de/solutions/it-security-solutions

Solarwinds-Hack

- MS Defender Erkennung seit 1.329.3680 „Trojan:MSIL/Solorigate.B!dha“
- Domain „avsvmcloud.com“ zu Killswitch umgebaut
- Achtung: Solarwinds empfahl in Vergangenheit Antivirus-Ausnahme

CAUSE

Anti Virus can cause file locking and application related issues such as polling related problems and web console issues.

RESOLUTION

For SolarWinds products, to prevent possible application related issues, unexpected behaviour and performance related problems, at minimum you would need to consider excluding the following items from antivirus or security software that you install on your SolarWinds Primary, Additional, HA backup polling engines and any web servers that you run.

Directories

- Exclude whole folders, including subdirectories,
- Check the correct syntax for the above that your security software supports as not all may be *.
- `Volume:\` is the volume you originally installed the product to.

Windows Server OS - 2019, 2016 (and 2012 R2 for old versions).

- `Volume:\Inetpub\SolarWinds\*`
- `Volume:\ProgramData\SolarWinds\*`
- `Volume:\Program Files (x86)\Common Files\SolarWinds\*`
- `Volume:\Program Files (x86)\SolarWinds\*`
- `Volume:\Windows\Temp\SolarWinds\*`
- `Volume:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\*`

Quelle: https://www.heise.de/news/I-f-SolarWinds-Backdoor-Hersteller-sorgte-fuer-Ausnahmen-von-AV-Ueberwachung-4990910.html

Agenda

- Lagebericht BSI und BKA
- Hardware-Lücken
- Solarwinds-Hack
- IT-Sicherheitsgesetz 2.0

IT-Sicherheitsgesetz 2.0

- IT-SIG 2.0 = Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- v1 im Juli 2015
- Entwurf für v2 am 16. Dezember 2020 beschlossen (130 Seiten)
- Inkrafttreten 2021 geplant
- Kritik an kurzer Zeit für Stellungnahmen (finale Version nur 27h)
- 1585 zusätzliche Planstellen in der Verwaltung
  → ca. 800 beim BSI

IT-Sicherheitsgesetz 2.0

- Portscans und Honeypots für Behörde erlaubt
- Speicherdauer Log-Dateien 12 Monate (statt 3)
- „Huawei-Klausel“ - Einsatz „kritischer Komponenten“
- IDS-Systeme für Kritis Betreiber verpflichtend
  Energieversorger auch umfasst
- Kritis-Meldepflichten zusätzlich für Unternehmen
  - mit besonderem öffentlichen Interesse (z.B. Rüstungsindustrie)
  - mit besonderer volkswirtschaftlichen Bedeutung
  - die der Störfallverordnung unterliegen
- Verbraucherschutz und -Information
  plus einheitliches IT-Sicherheitskennzeichen

Kongress findet erstmals online statt

Allianz für Cyber-Sicherheit
Partner

kostenlos Teilnehmer/Partner bei ACS werden

Vielen Dank für Ihre Aufmerksamkeit!

THOMAS KRENN®