Leibniz Universität Hannover

Allgemeine Bedrohungslage 2021 (2. Halbjahr)

Dr. Michael Brenner, LUIS

BSI-Lagebericht

- Laut Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die Gefährdungslage durch Cyberangriffe in Deutschland **angespannt bis kritisch.**

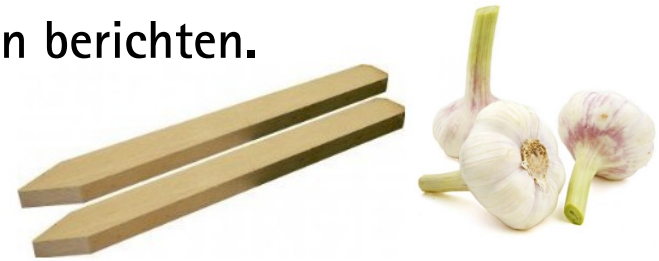
- Im Zuge der Corona-Pandemie haben Organisationen Millionen Arbeitsverhältnisse ins Homeoffice verlagert.

- In der akuten Krisensituation galt es, schnell zu handeln.

- Dabei kamen IT- und Datensicherheit häufig zu kurz.

„König der Schadsoftware“ Emotet zunächst zerschlagen

- Mittlerweile übersteigt die Zahl der weltweit bekannten Schadprogramme die Milliardengrenze.
- Im Berichtszeitraum von Juni 2020 bis Mai 2021 kamen rund 144 Millionen neue Varianten hinzu.
- Erst im Januar 2021 ist es im Rahmen einer internationalen Zusammenarbeit gelungen, die Emotet-Infrastruktur erfolgreich zu zerschlagen.
- **Wiederkehr im November 2021. Die Medien berichten.**



Neue Angriffsmethoden in der Pandemie

- Cyberkriminelle reagieren rasch auf gesellschaftlich relevante Themen und Trends und nutzen diese für gezielte Angriffe aus.
- In der Homeoffice-Situation nahmen insbesondere Identitätsdiebstähle zu. Beispielsweise gaben sich Hacker telefonisch als Servicekräfte aus.
- Cyberkriminelle setzen unter anderem auf Schadprogramme und bringen Organisationen aller Größen und Branchen in Bedrängnis.

Sparkasse

Wichtige Kundeninformation **Datum: 07.06.2020**

Sehr geehrte/r [redacted]

jüngste hat die Regierung der Bundesrepublik Deutschland ihr 130 Milliarden schweres Konjunkturpaket verabschiedet.

Dieses bringt für Sie als Endverbraucher unzählige Vorteile mit sich, wie z.B. der Erhöhung von Freibeträgen, Erstattungen und vieles mehr.

Der wohl größte Vorteil ist die Herabsetzung der Mehrwertsteuer von derzeit 19% auf zukünftig 16%.

Für eine Bank wie uns, bedeutet dies zweifelsohne auch gewissen Anpassungen in unseren Systemabläufen.

So werden beispielsweise die monatlichen Kontoführungsgebühren vorübergehend abgeschafft.

Wenn Sie von der Abschaffung profitieren möchten, folgen Sie bitte der unten angezeigten Schaltfläche und führen Sie die entsprechenden Schritte durch. Nach Abschluss des Vorgangs werden Ihnen automatisch die oben genannten Gebühren erlassen.

Weiter

Bitte beachten Sie, dass diese positiven Anpassungen befristet sind. Wir empfehlen Ihnen daher eine zeitnahe Durchführung.

Mit freundlichen Grüßen

Ihr Service-Team

Dies ist eine automatisch versendete Nachricht.
Bitte antworten Sie nicht auf dieses Schreiben, da die Adresse nur zu Versendung von E-Mails eingerichtet ist.

Neue Schadsoftware täglich

Durchschnittlicher täglicher Zuwachs neuer *Malware*-Varianten
Anzahl in Tausend

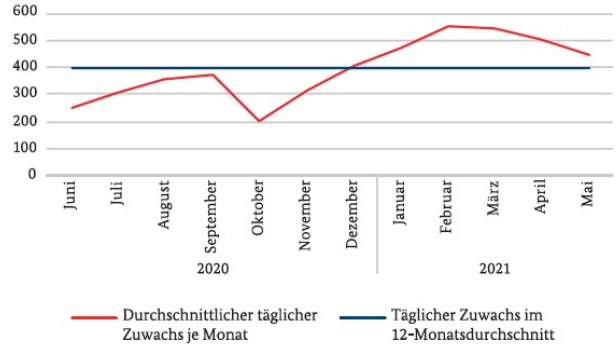


Abbildung 1: Täglicher Zuwachs neuer Schadprogramm-Varianten
Quelle: BSI-Auswertung von Rohdaten des Instituts AV Test GmbH

Neue Schadprogramm-Varianten
Anzahl in Millionen

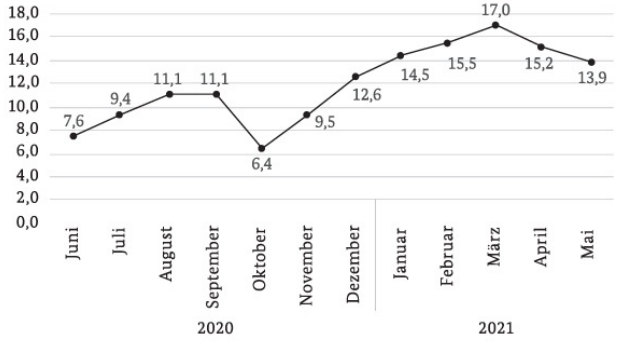


Abbildung 2: Neue Schadprogramm-Varianten
Quelle: BSI-Auswertung von Rohdaten des Instituts AV Test GmbH

Quelle: BSI

Keine Branche bleibt vor Angriffen verschont

- Laut des BSI geht die größte Gefahr nach wie vor von Angriffen mit Schadsoftware aus.

- Im Berichtszeitraum wurden unter anderem die Automobilindustrie, Flughäfen und Fluggesellschaften, mittelständische Unternehmen und Kommunalverwaltungen sowie Krankenhäuser und Hochschulen angegriffen.

- Einen starken Anstieg vermeldet das BSI erneut bei Sicherheitsvorfällen in Systemen der Kritischen Infrastruktur (KRITIS) mit Fokus auf den Gesundheits- und Energiesektor.

- Insgesamt bleibt die IT-Sicherheitslage im Berichtszeitraum angespannt bis kritisch (2020: angespannt).

Lage an der LUH

- Wiederkehrende gezielte Angriffe unterschiedlicher Art und Qualität
  - Emotet und andere Trojaner
  - CEO Fraud
  - Service-Staff Fraud
  - Diebstahl von Zugangsdaten
  - 9 meldepflichtige Datenschutzverstöße seit März 2020 (Phishing/Hacking)

- Allgemeine Bedrohungen 2021
  - FragAttack
  - Printnightmare
  - Exchange-Katastrophe
  - Racoon, SolarWinds, EMA-Angriff, ...

- Bisher kein vernichtender Angriff

„Wenn wir die Chancen der Digitalisierung nutzen wollen, müssen wir die Risiken beherrschbar machen."

Horst Seehofer, Bundesinnenminister

Quelle: BWI

Lage an der LUH in Zahlen

- Zeitraum 01.01.2021 – 17.11.2021
  - Schwachstelleninformationen DFN-CERT: 2570

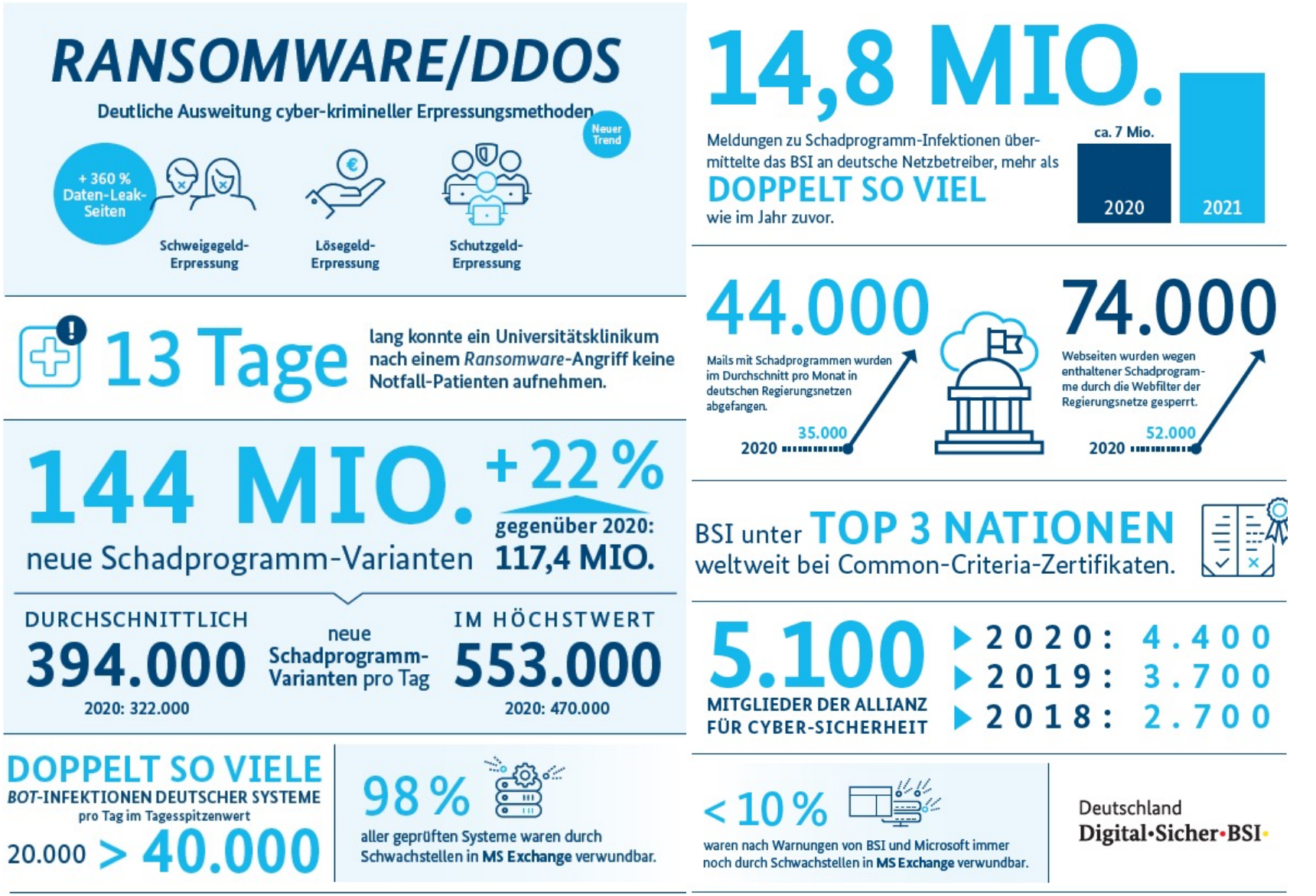
- Automatische Warnmeldungen (Ereignisse von IPs aus unserem Netzbereich):
  - 152
    - 54 aus den StwH-Wohnheimen
    - 56 aus WLAN/VPN
    - 40 LUH-IPs (Institute etc.)
    - 2 Eduroam-Gäste
  - Aufteilung
    - 97 Bot/HTTP
    - 27 Scan/Portscan
    - 15 Configuration / Unencrypted Communication
    - 9 Configuration / Unrestricted Access
    - 2 Attack/Virus
    - 1 Attack/Adware
    - 1 Configuration / Open resolver

Maßnahmen an der LUH

- Implementierung eines Informationssicherheits-Managementprozesses (siehe Folien von ISB Prof. Breitner)
- Stärkung des Organisationsaufbaus durch Benennung von dezentralen ISB (vollzogen)
- Personelle Verstärkung der strategischen (Herr Jens Rademacher) und operativen IT-Sicherheit (Ausschreibung läuft)
- Fortbestehen der ergriffenen technischen Maßnahmen.

Entwurf jährlicher Zyklus LUH ISMP

- Ende Januar/Juli:
  - Reguläre Sitzungen ISS (u.a. Überprüfung und Diskussion der LUH Ordnungen/Richtlinien (Januar) -> Template nötig)
- Ende März/September:
  - Reguläre Sitzungen ISS (u.a. LUIS IT-ST Report 2x p.a. -> Template nötig, DSB Report 2x p.a. -> Template nötig)
- Ende April/Oktober:
  - Reguläre Treffen mit dez. IS-Beauftragten bzw. FIOs (Report 2x p.a. -> Template nötig)
  - Jährlicher IS LUH Bericht (ca. 5 S. -> Template nötig) -> Präsidium (April)
- Mai/November:
  - Reguläre Sitzungen ISS (u.a. LUH Risikomanagement (-> Elspaß 30.6./31.12. -> Template nötig), Abstimmung/Input LUIS Sicherheits- bzw. Kundentagung, Abstimmung/Input Email LUH Präsident bzw. Awareness Kampagnen)
- Juni/Dezember:
  - Reguläre Treffen mit dez. IS-Beauftragten bzw. FIOs
- Berichte CISO und Diskussionen im BIT (6x p.a.)


RANSOMWARE/DDOS
Deutliche Ausweitung cyber-krimineller Erpressungsmethoden
Neuer Trend
+ 360 % Daten-Leak-Seiten
Schweigegeld-Erpressung
Lösegeld-Erpressung
Schutzgeld-Erpressung
13 Tage
lang konnte ein Universitätsklinikum nach einem *Ransomware*-Angriff keine Notfall-Patienten aufnehmen.
144 MIO.
neue Schadprogramm-Varianten
+22 %
gegenüber 2020: 117,4 MIO.
DURCHSCHNITTLICH
394.000
2020: 322.000
neue Schadprogramm-Varianten pro Tag
IM HÖCHSTWERT
553.000
2020: 470.000
DOPPELT SO VIELE
BOT-INFEKTIONEN DEUTSCHER SYSTEME
pro Tag im Tagesspitzenwert
20.000 > 40.000
98 %
aller geprüften Systeme waren durch Schwachstellen in MS Exchange verwundbar.
14,8 MIO.
Meldungen zu Schadprogramm-Infektionen übermittelte das BSI an deutsche Netzbetreiber, mehr als
DOPPELT SO VIEL
wie im Jahr zuvor.
ca. 7 Mio.
2020
2021
44.000
Mails mit Schadprogrammen wurden im Durchschnitt pro Monat in deutschen Regierungsnetzen abgefangen.
2020 35.000
74.000
Webseiten wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt.
2020 52.000
BSI unter TOP 3 NATIONEN
weltweit bei Common-Criteria-Zertifikaten.
5.100
MITGLIEDER DER ALLIANZ FÜR CYBER-SICHERHEIT
2020: 4.400
2019: 3.700
2018: 2.700
< 10 %
waren nach Warnungen von BSI und Microsoft immer noch durch Schwachstellen in MS Exchange verwundbar.
Deutschland Digital·Sicher·BSI·

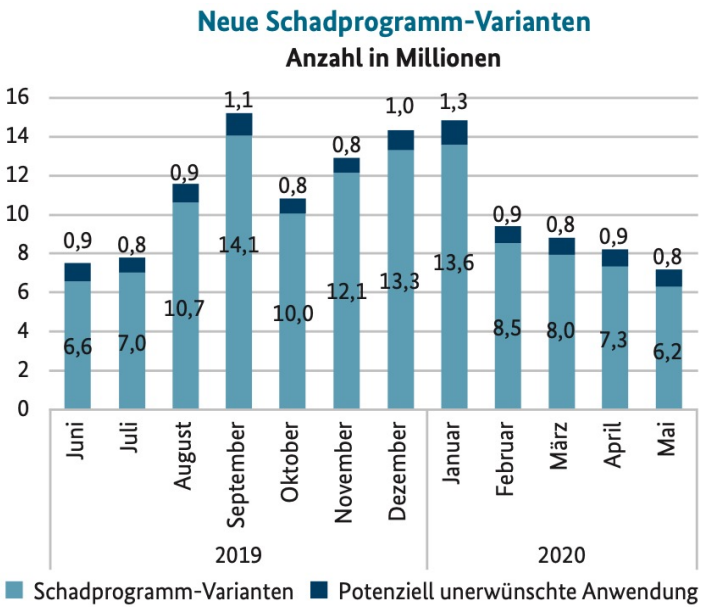
Quelle: BSI

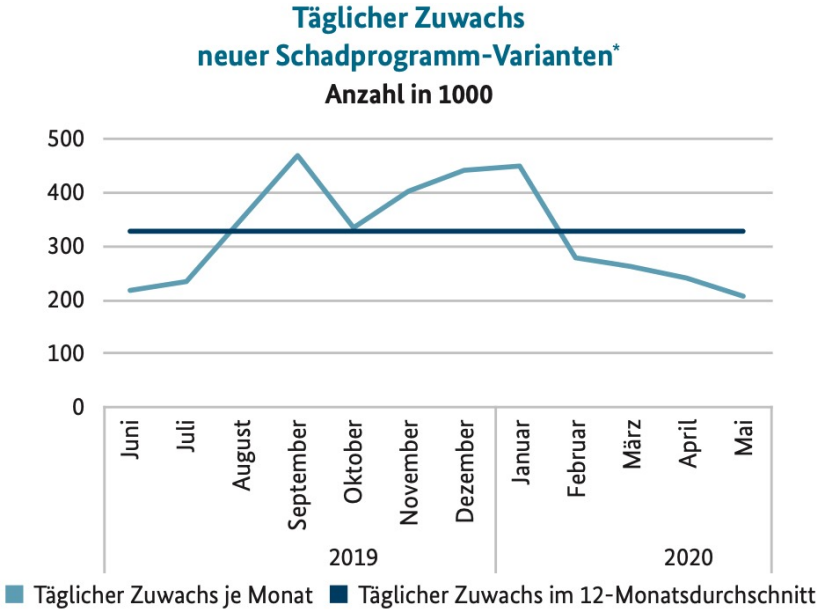
Vielen Dank für Ihre Aufmerksamkeit!

Dr. Michael Brenner

brenner@luis.uni-hannover.de

Schadsoftware 2020

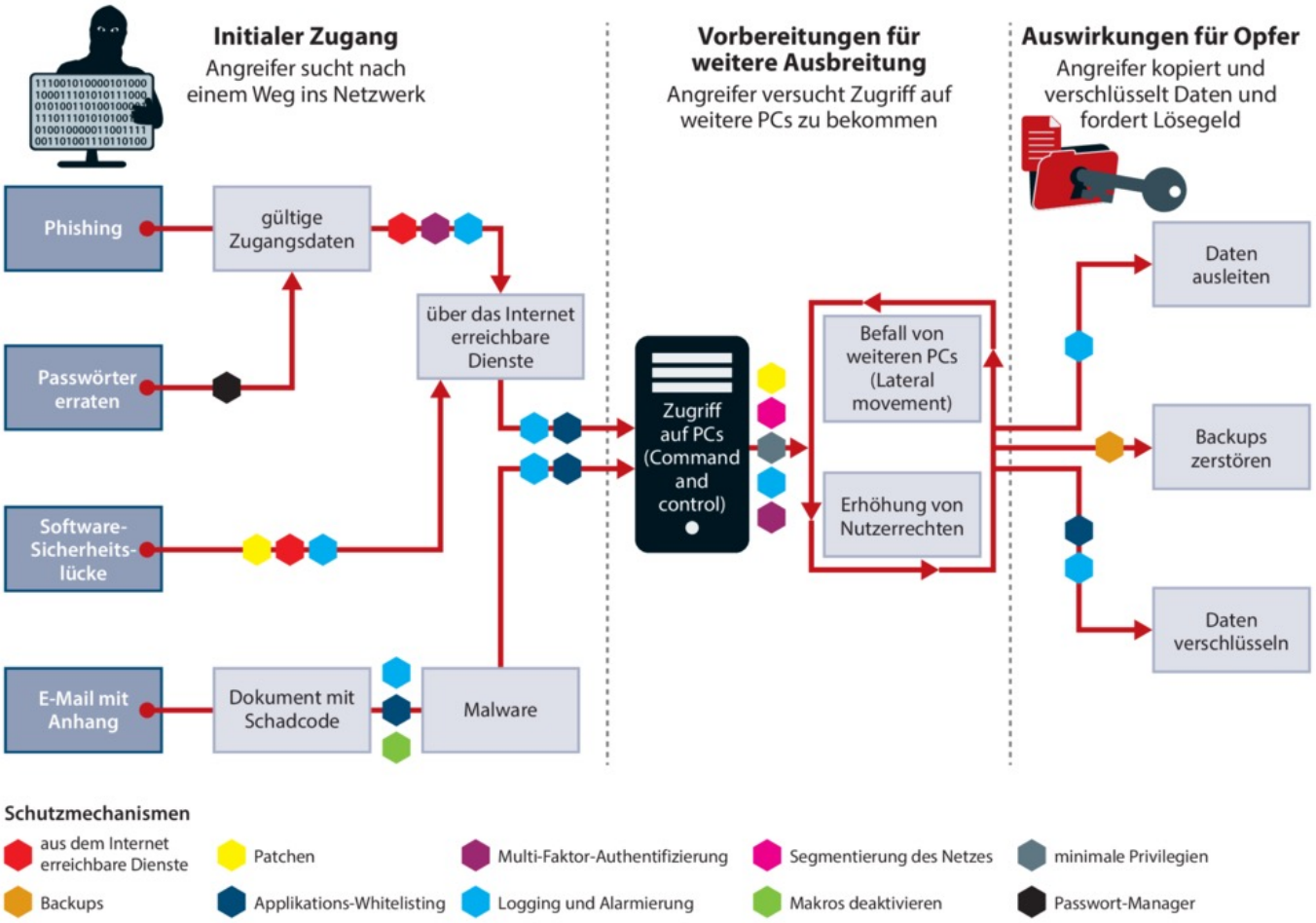




Quelle: BSI

So verläuft eine Ransomware-Attacke

In dieser Grafik vom CERT aus Neuseeland sieht man, wie Online-Kriminelle bei einer typischen Ransomware-Attacke auf Unternehmen vorgehen und was Sie dagegen tun können. Während der verschiedenen Stadien einer Attacke gibt es jeweils andere Sicherheitskonzepte, um Systeme effektiv zu schützen. Admins sollten das Schaubild genaustens studieren und auf die IT-Infrastruktur ihres Unternehmens anwenden. Im Anschluss sollte klar werden, welche Schwächen das eigene Sicherheitskonzept hat und mit welchen Maßnahmen Sie dagegen steuern können.



Quelle: BSI

FragAttack WLAN-Schwachstellen

Leibniz Universität Hannover

BSI Meldung am 11.05.2021 (orange)

Unter der Bezeichnung "FragAttacks" (fragmentation and aggregation attacks) veröffentlichten Sicherheitsforscher am Dienstag, den 11. Mai 2021, Erkenntnisse zu zahlreichen WLAN-Schwachstellen, die sowohl WLAN-Router als auch die damit verbundenen Geräte betreffen können. Nach derzeitiger Sachlage ist davon auszugehen, dass einige der Sicherheitslücken designbedingt im Wi-Fi-Standard vorliegen und somit herstellerübergreifend ausgenutzt werden können. Die verwendete Verschlüsselungstechnik spielt für Attacken ebenfalls keine Rolle. Ferner führen die Sicherheitsforscher aus, dass jedes von ihnen getestete WLAN-Gerät von mindestens einer der genannten Schwachstellen betroffen ist. https://www.fragattacks.com

Bewertung

Zum aktuellen Zeitpunkt ist davon auszugehen, dass nur eine lokale Ausnutzung der Schwachstellen möglich ist – also dann, wenn sich ein Angreifer in Reichweite eines Access Points oder Endgeräts eines potenziellen Opfers befindet. Gleichzeitig stellt die mögliche Betroffenheit zahlreicher – ggf. sogar aller – WLAN-Geräte ein erhebliches Risiko für Betreiber und Nutzer dar.

FragAttack WLAN-Schwachstellen

Leibniz Universität Hannover

Maßnahmen

Das BSI empfiehlt, umgehend Herstellerwebseiten entsprechend der eingesetzten WLAN-Komponenten auf Informationen zu diesem Sachverhalt zu prüfen und bereitgestellte Patches zeitnah zu installieren. Die Installation sollte unter Beachtung des Ergebnisses einer Risikoanalyse durchgeführt werden. Bislang ungepatchte Schwachstellen in den Geräten müssen im Zusammenhang mit diesem Sachverhalt neu bewertet werden, da sich durch die potenzielle Umgehung der Verschlüsselung ggf. eine geänderte Bedrohungslage und damit ein geändertes Risiko ergibt.

Lage in der LUH

500 der installierten APs ohne verfügbaren Patch

200 APs können kurzfristig (1 Jahr) ersetzt werden

DFN-CERT: Keine substanziellen Angriffe bekannt

Risiko ist auch aufgrund der erforderlichen Nähe zu einem angegriffenen AP zeitlich begrenzt vertretbar

Etliche nds. Unis haben noch keine Maßnahmen ergriffen

Printnightmare Fehler im Spoolerservice

In den vergangenen Monaten gab es mehrere Sicherheitslücken (CVE-2021-1675, CVE-2021-34527, CVE-2021-34481, CVE-2021-36958), die unter dem Namen Printnightmare zusammengefasst werden. Diese wurden teils aktiv ausgenutzt, bevor Microsoft einen Patch veröffentlicht hatte. Betroffen war unter anderem die Kreisverwaltung Anhalt-Bitterfeld in Sachsen-Anhalt. Dort wurde ein Server über die Sicherheitslücke gehackt und anschließend per Ransomware die Daten verschlüsselt.

Lage an der LUH

LUIS News-Meldung am 2.7.

Bis zur Auslieferung des Patches Empfehlung: Deaktivierung des Drucker-Spoolers

Patch verlief chaotisch, erst im September gefixt

Keine bekannten Schäden durch Ausnutzung der Schwachstelle an der LUH

Emotet, Portscans und weitere Themen

Postscans

- Vermehrte Registrierung von externen Portscans
- Keine akute Gefahr, wird aber protokolliert

Übernahme von Windows Infrastruktur durch LUIS

- Steigende Anzahl von Anfragen zum Betrieb von Windows Infrastruktur durch LUIS seitens LUH Einrichtungen
- Auch auf gestiegenes Sicherheitsbewusstsein zurückzuführen
- Mit dem iw-Exchange wird demnächst die letzte große dezentrale Exchange-Installation ins LUIS verlagert

Emotet

- In letzter Zeit keine bekannt gewordenen Angriffe
- In Sicherheitskreisen werden durchaus vergleichbare Angriffe für die Zukunft erwartet
- Software und Infrastruktur-Blaupausen für die „wirtschaftliche" Verwertung existieren
- Maßnahmen der LUH (z. B. Blockieren aktiver E-Mail-Anhänge) bleiben in Kraft