Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Aktuelle Cyber-Bedrohungslage

Dirk Häger
BSI

PITS 2024

Tagträumereien

ISMS hervorragend umgesetzt:

- Alle Mitarbeitenden sind „aware“
- Die Patchprozesse sind hochautomatisiert
- Keine Legacy-Systeme im Einsatz

Tagträumereien

ISMS hervorragend umgesetzt:

- Alle Mitarbeitenden sind „aware“
- Die Patchprozesse sind hochautomatisiert
- Keine Legacy-Systeme im Einsatz

Einfallsvektoren für Angreifer

- Bösartige Mail-Anhänge
- Phishing-Mails (SMS, Anrufe, ...)
- Drive by Downloads
- Cross Site Scripting
- Schwache Passwörter

- Ungepatchte Schwachstellen
- Fehlkonfigurationen

- „Das Restrisiko“

Restrisiko??????


citrix
Progress MOVEit
Microsoft
CISCO
FORTINET
Kaseya
ivanti
CHECK POINT
SOLARWINDS
AnyDesk

VPN-Gateways wirklich ein Problem? (1/2)

Hackers targeting VPN vulnerabilities in ongoing attacks

As remote work increased during the pandemic, threat actors increasingly targeted known vulnerabilities.

By **Arielle Waldman,** News Writer

Published: **26 Apr 2021**

Nation-state actors are exploiting known vulnerabilities in several VPN and remote access products, indicating a troubling trend for enterprises.

VPN-Gateways wirklich ein Problem? (2/2)

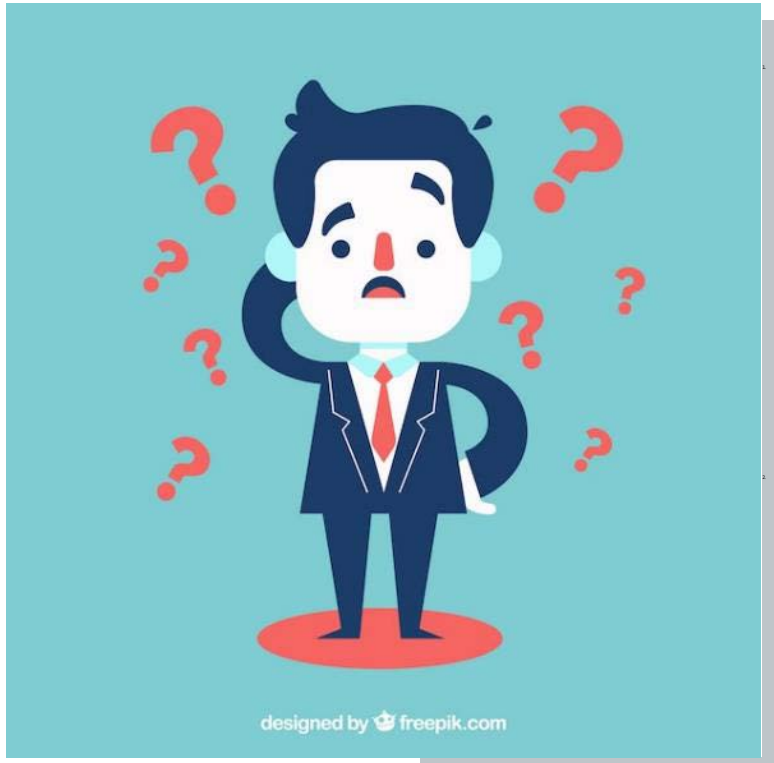
- **314 VPN vulnerabilities** have been disclosed since 2021
  - **2023**: 133 VPN vulnerabilities disclosed with an average base score of 7.35
  - **2022**: 93 VPN vulnerabilities disclosed, average base score of 7.52
  - **2021**: 88 VPN vulnerabilities disclosed, average base score of 7.46
- At least 20 vulnerabilities are known to have been exploited, according to CISA.

Quelle: https://www.top10vpn.com/research/vpn-vulnerabilities/ (United States National Vulnerability Database)

Aktuelle Check Point Schwachstelle

- Anfang letzter Woche: ca. 1700 verwundbare Systeme in Deutschland
- Täter ursprünglich vermutlich State Actor: nun viele Trittbrettfahrer
- Angriff möglich auf Scriptkiddieniveau
  - ```
    POST /clients/MyCRL HTTP/1.1
    Host: <redacted>
    Content-Length: 39

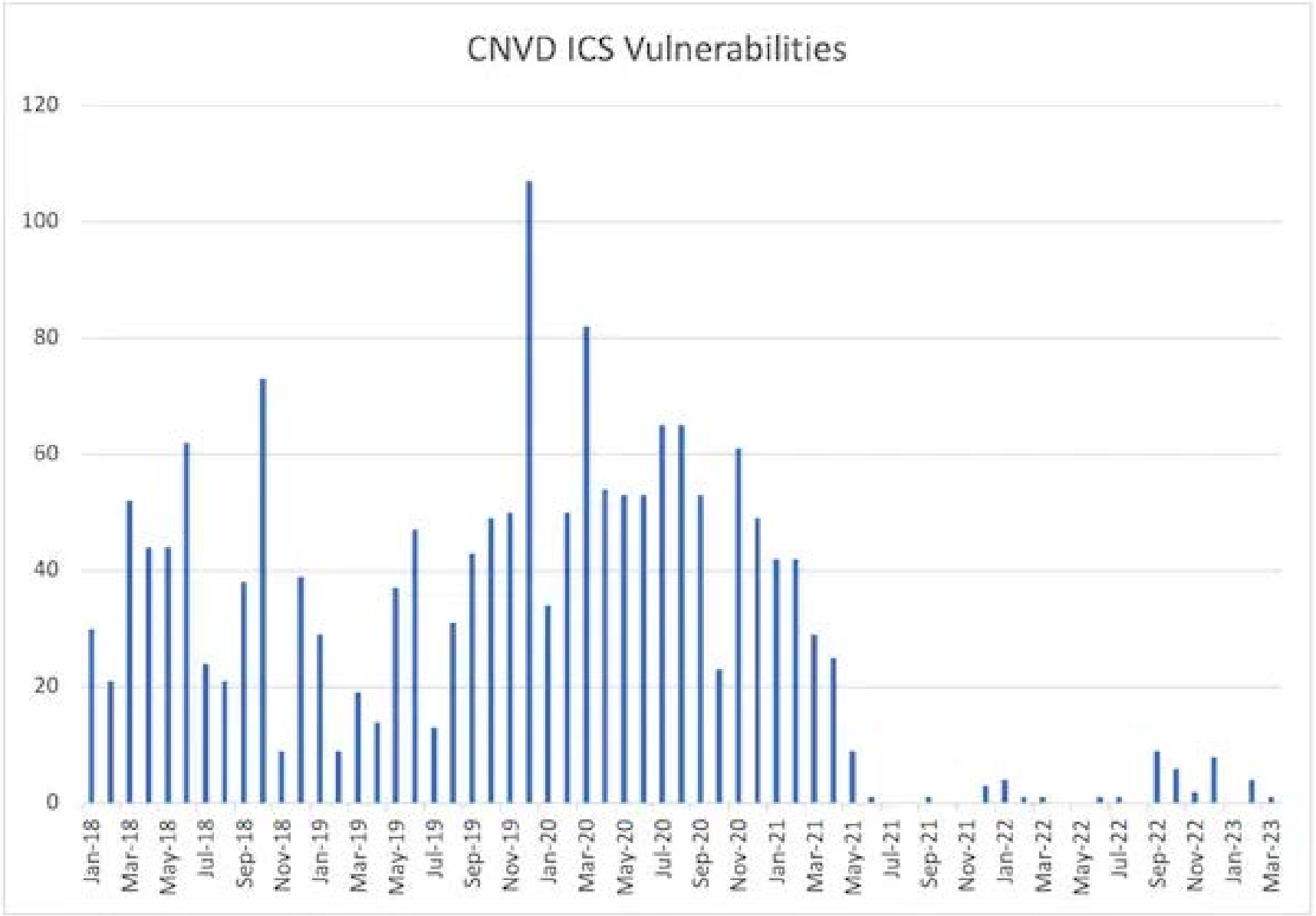
    aCSHELL/../../../../../../../etc/shadow
    ```
- Webserver mit Root-Rechten
- Hashes teilweise MD5
- CC-Zertifikat mit EAL 4


    ```

Was tun gegen 0days in VPN-Gateways?

- Detektion und Reaktion ein **MUSS** („Backup != Cyber Recovery“, …)
- Netzwerkdesign: Remote Access nicht direkt zu den Kronjuwelen (Segmentierung)
- Regularien für Home Office (Zeiten)
- Professionalisierung der IT (Managed Services, Cloud)

- Keine einfachen Lösungen, sondern **AUFWÄNDIG**


CNVD ICS Vulnerabilities
120
100
80
60
40
20
0
Jan-18
Mar-18
May-18
Jul-18
Sep-18
Nov-18
Jan-19
Mar-19
May-19
Jul-19
Sep-19
Nov-19
Jan-20
Mar-20
May-20
Jul-20
Sep-20
Nov-20
Jan-21
Mar-21
May-21
Jul-21
Sep-21
Nov-21
Jan-22
Mar-22
May-22
Jul-22
Sep-22
Nov-22
Jan-23
Mar-23

Ausblick

- NIS 2
- Cyber Resilience Act: mehr Pflichten für Hersteller
- SBOM + CSAF
- BISP (Customer Portal)
- Mehr aktive Maßnahmen

Vielen Dank für Ihre Aufmerksamkeit!

Dirk Häger
Abteilungsleiter OC
dirk.haeger@bsi.bund.de
Tel. +49 (0) 22899 9582-5304
Fax +49 (0) 22899 109582-5304

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Abteilung OC
Godesberger Allee 185-189
53175 Bonn

Bundesamt
für Sicherheit in der
Informationstechnik