FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Agenda

Digital Innovation Hub Süd Klaus Gebeshuber | Vorstellung DIH, IT Sec Talks für KMU

Aktuelle Bedrohungen für Unternehmen im Jahr 2021 Klaus Gebeshuber – FH JOANNEUM

Forschungsprojekte in der IT-Sicherheit Christian Derler – JOANNEUM Research

Fahrzeuge als Ziel für Hacker Markus Wolf - AVL | Fahrzeuge als Ziel für Hacker

Schwerwiegende Linux Sicherheitslücke in sudo Patrick Staubmann – FH JOANNEUM

Advanced WEB Attacks - HTTP Request Smuggling Manuel Hacker – FH JOANNEUM

| |

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

DIH-SÜD – Digital Innovation Hub Süd

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

DIH SÜD - Digital Innovation Hub Süd

Was ist der DIH SÜD?

Der **Digital Innovation Hub Süd** ist ein nicht-wirtschaftlich tätiges Kompetenznetzwerk, das als Koordinations- und Anlaufstelle für Selbstständige und Unternehmen zum Thema Digitalisierung im Raum Süd-Österreich dient.

Unser Ziel ist es Digitalisierung in KMU zu ermöglichen, indem wir:

- Bewusstsein für digitale Herausforderungen und Chancen schaffen
- bestehendes Angebot einfach kommunizieren und zugänglich machen
- Anwender und Anbieter zusammenbringen
- spannende Projekte initiieren
- Wissenstransfer zwischen F&E und Wirtschaft fördern.

https://www.dih-sued.at/

FFG Forschung wirkt.
Das Land Steiermark
LAND KÄRNTEN

DIH SÜD - Digital Innovation Hub Süd

https://www.dih-sued.at/

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

DIH SÜD

- Angebot der FH JOANNEUM/IIT
  - Security Infoveranstaltungen
  - IT-SEC Talks für KMU
  - Penetration Testing Trainings

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Rückblick 2020/2021

02/2020 – Toll Group - Ransomware

40.000 Employees
50 Countries

02/2020 MailTo

05/2020 Netfilim
220GB data stolen

03/2020 – Mariott Data Breach – 5.2Mio records

18.4 Mio £ Fine

07/2020 Garmin - Ransomware

Monday, 27 July 2020, 12:30 pm CDT

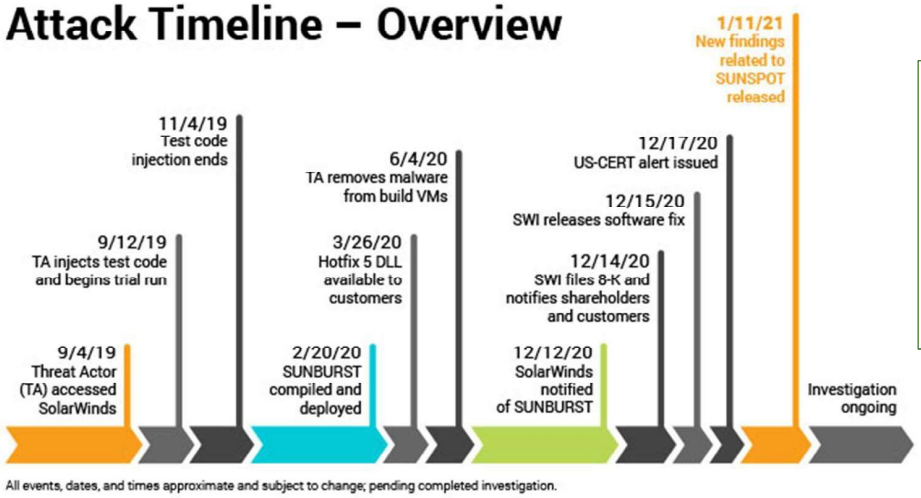
Garmin issues statement on recent outage

Payed?

Affected systems are being restored and normal operation is expected soon

OLATHE, Kan.–(BUSINESS WIRE)–
Garmin® Ltd. (NASDAQ: GRMN), today announced it was the victim of a cyber attack that encrypted some of our systems on July 23, 2020. As a result, many of our online services were interrupted including website functions, customer support, customer facing applications, and company communications. We immediately began to assess the nature of the attack and started remediation. We have no indication that any customer data, including payment information from Garmin Pay™, was accessed, lost or stolen. Additionally, the functionality of Garmin products was not affected, other than the ability to access online services.

12/2020 FireEye / Solar Winds



18.000 Customer
Cisco
Microsoft
Intel
Nvidia,
VMWare
AT&T,
Malwarebytes
Crowdstrike,
FireEye,...

01-03/2021 HAFNIUM - Microsoft Exchange

March 2, 2021

HAFNIUM targeting Exchange Servers with 0-day exploits

Microsoft Threat Intelligence Center (MSTIC)
Microsoft 365 Defender Threat Intelligence Team
Microsoft 365 Security

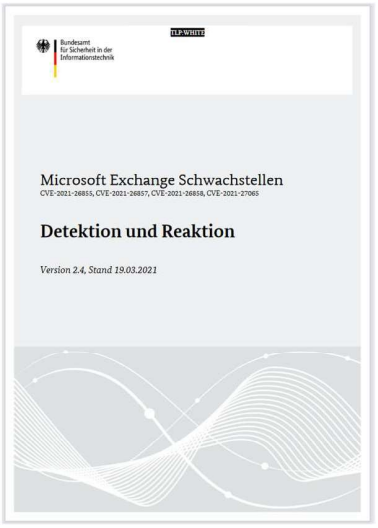
Who is HAFNIUM?

HAFNIUM primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.

HAFNIUM has previously compromised victims by exploiting vulnerabilities in internet-facing servers, and has used legitimate open-source frameworks, like Covenant, for command and control. Once they've gained access to a victim network, HAFNIUM typically exfiltrates data to file sharing sites like MEGA.

In campaigns unrelated to these vulnerabilities, Microsoft has observed HAFNIUM interacting with victim Office 365 tenants. While they are often unsuccessful in compromising customer accounts, this reconnaissance activity helps the adversary identify more details about their targets' environments.

HAFNIUM operates primarily from leased virtual private servers (VPS) in the United States.



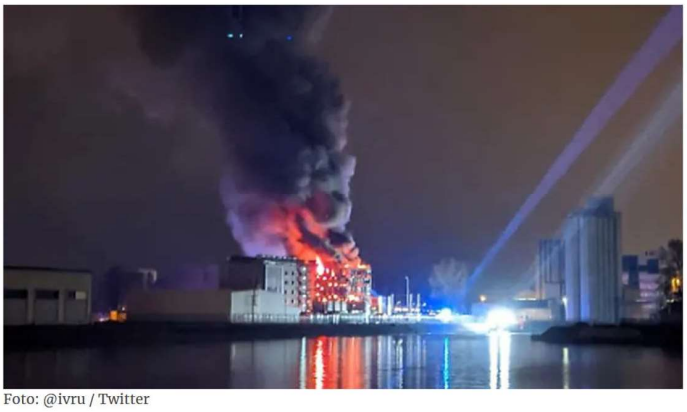
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf?__blob=publicationFile&v=6
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

01-03/2021 HAFNIUM - Microsoft Exchange

- **Jan. 5:** DEVCORE alerts Microsoft of its findings.
- **Jan. 6:** Volexity spots attacks that use unknown vulnerabilities in Exchange.
- **Jan. 8:** DEVCORE reports Microsoft had reproduced the problems and verified their findings.
- **Jan. 25:** DEVCORE snags proxylogon.com, a domain now used to explain its vulnerability discovery process.
- **Jan. 27:** Dubex alerts Microsoft about attacks on a new Exchange flaw.
- **Jan. 29: Trend Micro** publishes a blog post about "**China Chopper**" web shells being dropped via Exchange flaws (but attributes cause as Exchange bug Microsoft patched in 2020)
- **Feb. 2:** Volexity warns Microsoft about active attacks on previously unknown Exchange vulnerabilities.
- **Feb. 8:** Microsoft tells Dubex it has "escalated" its report internally.
- **Feb. 18:** Microsoft confirms with DEVCORE a target date of Mar. 9 (tomorrow) for publishing security updates for the Exchange flaws. That is the second Tuesday of the month — a.k.a. "**Patch Tuesday**," when Microsoft releases monthly security updates (and yes that means check back here tomorrow for the always riveting Patch Tuesday roundup).
- **Feb. 26-27:** Targeted exploitation gradually turns into a global mass-scan; attackers start rapidly backdooring vulnerable servers.
- **Mar. 2:** A week earlier than previously planned, Microsoft releases updates to plug 4 zero-day flaws in Exchange.
- **Mar. 3:** Tens of thousands of Exchange servers compromised worldwide, with thousands more servers getting freshly hacked each hour.
- **Mar. 4:** White House National Security Advisor **Jake Sullivan** tweets about importance of patching Exchange flaws, and how to detect if systems are already compromised.
- **Mar. 5, 1:26 p.m. ET:** In live briefing, White House press secretary **Jen Psaki** expresses concern over the size of the attack.
- **Mar. 5, 4:07 p.m. ET:** KrebsOnSecurity breaks the news that at least 30,000 organizations in the U.S. — and hundreds of thousands worldwide — now have backdoors installed.
- **Mar. 5, 6:56 p.m. ET:** Wired.com confirms the reported number of victims.
- **Mar. 5, 8:04 p.m. ET:** Former CISA head **Chris Krebs** tweets the real victim numbers "dwarf" what's been reported publicly.
- **Mar. 6:** CISA says it is aware of "widespread domestic and international exploitation of Microsoft Exchange Server flaws."
- **Mar. 7:** Security experts continue effort to notify victims, coordinate remediation, and remain vigilant for "Stage 2" of this attack (further exploitation of already-compromised servers).
- **Mar. 9:** Microsoft says 100,000 of 400,000 Exchange servers globally remain unpatched.
- **Mar. 9:** Microsoft "Patch Tuesday," (the original publish date for the Exchange updates); Redmond patches 82 security holes in Windows and other software, including a zero-day vulnerability in its web browser software.
- **Mar. 10:** Working exploit for Exchange flaw published on Github and then removed by Microsoft, which owns the platform.
- **Mar. 10:** Security firm ESET reports at least 10 "advanced persistent threat" (APT) cybercrime and espionage groups have been exploiting the newly-exposed Exchange flaws for their own purposes.

https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/

03/2021 OVH Rechenzentrum



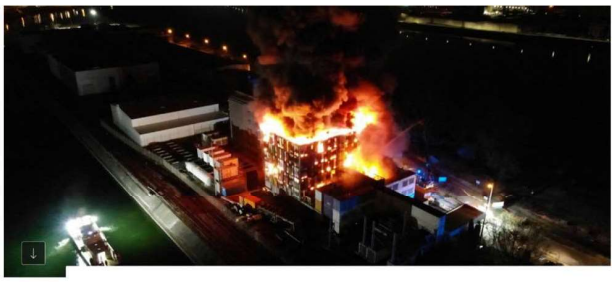


Foto: @ivru / Twitter

Der Standort des Cloudanbieters wurde offline genommen. Auch andere Dienste von OVHcloud haben Probleme, zahlreiche europäische Websites waren down.

https://www.inside-it.ch/de/post/brand-zerstoert-ovh-rechenzentrum-in-strassburg-20210310
https://www.faz.net/aktuell/feuilleton/medien/groesstes-rechenzentrum-europas-brennt-komplett-nieder-17241629.html

04/2021 Alba Ransomware

Alba wehrt sich gegen Hacker

Gegen Fertigungsspezialist liegt Forderung von Erpressern vor. Angriff legte Teile des Betriebes in Forstau mit vielen steirischen Beschäftigten eine Woche lahm.

Von Veronika Höflehner

Der Fertigungsspezialist Alba an der steirischen Landesgrenze in der Forstau (Radstadt) wurde Opfer eines Cyberangriffes. Dieser hat in der Nacht vom 6. auf den 7. April das gesamte Netzwerk lahmgelegt. Seither arbeitet man mit einer externen Firma fieberhaft an der Wiederherstellung der Systeme. Wie die Salzburger Polizei bestätigt, liegt eine Erpressungsforderung vor, die Ermittlungen laufen. Zur Schadenssumme ist nichts bekannt. Im Unternehmen, das Dutzende Personen aus dem Raum Schladming beschäftigt, werden hochkomplexe Werkzeuge, Maschinen und Anlagen gefertigt. Eine Firmensprecherin bestätigte den Cyberangriff. Genauere Auskünfte gab es aus ermittlungstaktischen Gründen aber nicht. Laut informierten Kreisen verbreitete sich eine eingeschleuste Software langsam im Netzwerk, alle damit verbundenen Geräte waren nicht mehr bedienbar.

Die Maschinenbaukonstrukteure in der Forstau mussten deshalb ihre Arbeit rund eine Woche lang niederlegen. Der Vertrieb wich zur Kommunikation mit den Kunden auf alternative E-Mail-Adressen aus, hieß es aus dem Mitarbeiterumfeld. Die Produktion, also das händische Zusammenbauen der Teile, lief aber weiter. Alle Alba-Mitarbeiter wurden angehalten, ihre bisher noch unabgetasteten Computer nicht mit dem Netzwerk zu verbinden. Die „Alba tooling & engineering GmbH" ist eine Salzburger Firmengruppe in Familienbesitz mit weltweit 400 Mitarbeiterinnen und Mitarbeitern. Als eines der wenigen Industrieunternehmen der Region arbeiten dort auch viele Einstaler. Das Unternehmen hat seinen Hauptsitz in der Forstau und insgesamt acht Standorte, unter anderem in Osteuropa, Indien, China und den USA. Zu den Kunden zählen die Automobilindustrie, aber auch die Luftfahrt-, Schiffbauwirtschaft, Elektro- und Baubranche sowie Möbel- und Textilindustrie.

Alba-Standort in Forstau an der salzburgisch-steirischen Grenze

Bei einem Angriff

Wird ein Unternehmen Opfer eines Cyberangriffs, rät das Innenministerium zur Anzeige bei der Polizei. Alle Sachverhalte im Zusammenhang mit Ransomware werden im Bundeskriminalamt vom Cybercrime Competence Center bearbeitet.

START-UP PILZKISTE

01/2021 Palfinger Ransomware

WEGEN CYBERATTACKE

Palfinger zahlte Geld an Erpresser

Nur mit der Zahlung von Lösegeld konnte der Salzburger Kranhersteller Palfinger Ende Jänner eine Cyberattacke abwehren. Der Angriff hatte das Unternehmen gelähmt. Wie viel Geld an die Erpresser gezahlt wurde, sagt Palfinger aber nicht.

PALFINGER

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

05/2021 Colonial Pipeline US - Ransomware

DarkSide (RU)

Ransom:
- 75 Bitcoins paid – 4,4Mio$
- 63,7 Bitcoins recovered – 2,4Mio$

Initial Attack:
- Reused VPN credentials

https://en.wikipedia.org/wiki/Colonial_Pipeline_cyber_attack

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security