IT security & data security in practice

Dr. Stefan Hofbauer

CIS Compliance Summit 2023

19.09.2023

Top Bedrohungen ENISA

- ENISA Threat Landscape 2022
  - Ransomware
  - Malware
  - Social Engineering Threats
  - Threats against data
  - Threats against availability (DoS, Internet threats)
  - Disinformation – misinformation
  - Supply-chain attacks

  - + Phishing (Social Engineering)
  - + Software Vulnerabilities
  - + Datenverlust (Threats against data)

Cyber-Angriffe 2023 (Auszug)

Security

Cyberangriff bei ABB: "Der Vorfall wurde erfolgreich eingedämmt"

26.05.2023 Lesezeit: ca. 2 Minuten #ABB #Cyber Security

Der Schweizer Industriekonzern ABB wurde Opfer eines Hacker-Angriffs. Die russische Gruppe "Black Basta" setze dabei auf "doppelte" Erpressungsversuche. Zuletzt gab das Unternehmen Entwarnung, auch wenn längst nicht alle Punkte geklärt wurden.

Der Schweizer Technologiekonzern ABB wurde am 7. Mai Opfer eines Hackeragriffs. Der IT-Sicherheitsvorfall hatte Auswirkungen auf bestimmte Systeme, wie das Unternehmen verlautbaren ließ. Es wurden eine Untersuchung eingeleitet, Spezialisten engagiert und bestimmte Strafverfolgungs- und Datenschutzbehörden informiert. Zudem soll es noch weitere Massnahmen gegeben haben, um den Vorfall einzudämmen und zu beurteilen. "Der Vorfall wurde nun erfolgreich eingedämmt", lautete das letzte Update von ABB am 23. Mai. Dementsprechend seien alle wichtigen Services und Systeme sowie alle Fabriken in Betrieb, Kund:innenanliegen werden bearbeitet. Das Unternehmen verbessert laut Aussendung die Sicherheit seiner Systeme weiter. Bei Bedarf werde sich das Unternehmen mit betroffenen Parteien in Verbindung setzen, etwa mit bestimmten Kunden, Lieferanten und/oder Einzelpersonen, deren persönliche Daten betroffen waren.

Doch DDoS-Angriff auf MS-Cloud (5.–14. Juni 2023) für Ausfälle verantwortlich

Publiziert am 17. Juni 2023 von Günter Born

[English]Seit dem 5. Juni 2023 gab es ja immer wieder Probleme mit der Verfügbarkeit der Microsoft-Cloud bzw. der dort angebotenen Dienste. Ich hatte in meinen Blog-Beiträgen spekuliert, dass da wohl ein Angriff hinter stecken könnte, zumal eine Hacktivisten-Gruppe Anonymous Sudan die behauptet hatte. Aus Microsoft-Kreisen hieß es uniso "nichts bekannt". Nun liegt mir ein Post Incident Report For Microsoft 365 vor, als dem man ableiten kann, dass es DDoS-Angriffe auf Microsofts Cloud gegeben haben muss.

Anzeige

Microsoft-Cloud mehrfach gestört

Als ich am 5. Juni 2023 über eine Störung bei Microsoft Exchange Online informiert wurde, ging ich noch von einem technischen Problem aus – obwohl ich im Beitrag Exchange Online-Störung (5. Juni 2023) – Werk russischer Hacker? bereits die Frage stellte, ob Hacker dahinter stecken können. Grund war, dass eine Hacktivsten-Gruppe mit dem Namen Anonymous Sudan die Verantwortung für die Störung reklamierte.

CyberNews
@CyberNews

Microsoft #Outlook was down for thousands of American users after pro-Russian #hacktivist group #AnonymousSudan claims to have started a new campaign dedicated to targeting US companies and infrastructure.
#cybersecurity #infosec #Microsoft
Tweet übersetzen

Hacker versuchten Cyber-Attacke auf Uni Graz

Der Angriff wurde am Freitag bei einem Routine-Check entdeckt. Es dürften keine Daten gestohlen worden sein.

06.02.2023, 11:11

Kommentare Teilen

Hacker haben am Wochenende einen Cyberangriff auf die Universität Graz versucht. Der Angriff auf die IT-Infrastruktur ist nach Angaben der Universität beim routinemäßigen Sicherheitscheck durch den Informatikdienst der Universität festgestellt worden.

Nach bisherigem Wissensstand dürften keine Daten verschlüsselt oder abgesaugt worden sein. Externe IT-Forensiker sind zur Analyse beigezogen worden, teilte die Pressestelle auf APA-Anfrage mit.

Systeme heruntergefahren

Der Angriff am vergangenen Freitag dürfte über verschiedene IT-Systeme der Uni Graz erfolgt sein. Am Wochenende wurden die IT-Systeme der Universität in weiten Teilen heruntergefahren - zahlreiche Mitarbeiter und Studierende konnten nicht auf ihr Online-System zugreifen.

Am Montag standen die IT-Systeme den Universitätsangehörigen wieder zur Verfügung. Es muss jedoch aus Sicherheitsgründen jederzeit und länger mit Einschränkungen verschiedener Systeme bzw. Dienste gerechnet werden.

IM DARKNET AUFGETAUCHT

Magenta: Hackerangriff auf 20.000 Kundendaten

Österreich | 01.02.2023 17:57

(Bild: dpa/Oliver Berg (Symbolbild))

Russische Hacker haben einen Hackerangriff auf einen externen österreichischen Vertriebspartner von Magenta Telekom verübt: 20.000 Kundendaten tauchten in der Folge im Darknet auf. Betroffen seien Daten aus dem Zeitraum 2020 bis 2022, teilte das Unternehmen am Mittwochabend mit. Magenta erhielt am Dienstag davon Kenntnis, Polizei und Datenschutzbehörde wurden eingeschaltet. Forderungen der Hacker gab es bislang nicht, hieß es.

Cyberspionage

Chinesische Hacker greifen Bundesbehörde an

von Marcel Rosenbach und Hakan Tanriverdi 31.08.2023 16:15 Uhr

Hacker, die mutmaßlich für Chinas Regierung arbeiten, konnten das Netzwerk des Bundesamtes für Kartographie infiltrieren. Dafür nutzen sie auch Computer von privaten Nutzern.

Die Hacker nutzten für ihre Angriffe Internetanschlüsse von Privatnutzern aus Deutschland. (Symbolbild)

Quelle: Imago

Hacker nahmen deutsche Finanzaufsicht ins Visier

Online seit: 4. September 2023

Deutsche Finanzaufsicht von Hackern angepeilt © APA/AFP/NICOLAS ASFOURI

Die deutsche Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ist Opfer eines Angriffs aus dem Internet geworden. Die Server der Behörde seien Ziel eines „Distributed Denial of Service"-Angriffs (DDoS), sagte ein BaFin-Sprecher am Montag. Seit Freitag sei die BaFin-Webseite daher nicht oder nur eingeschränkt erreichbar.

Die IT-Abteilung arbeite fieberhaft an der Abwehr der Attacke, die sich auf den Internetauftritt beschränke. Wann alles wieder normal laufe, lasse sich bisher aber noch nicht abschätzen. Zunächst hatte der „Spiegel" über den Vorfall berichtet.

HACKERANGRIFF

Großangelegter Hackerangriff in Italien traf auch Ministerien

Am Freitag war das IT-System des Industrieministeriums nicht zugänglich, am Mittwoch wurde ein Onlineportal des Innenministeriums blockiert

26. Mai 2023, 14:34 2 Postings

Am Mittwoch hatten sich Hacker (Symbolbild) der Gruppe NoName057(16) zu dem Angriff auf das Portal des Innenministeriums bekannt.

Computersysteme lahmgelegt

Cyberangriffe auf ATU-Kette und Medienportale

19.05.2023 16:04 Uhr

Die Werkstattkette ATU meldet Probleme infolge von Angriffen auf die IT-Infrastruktur. Die Polizei ermittelt. Auch bei Medienportalen gibt es Ausfälle nach Hackerangriffen.

Die Polizei ermittelt nach Hackerangriffen auf die Werkstattkette ATU. (Archivbild)

Quelle: dpa

CHRONIK

Fortschritte nach Hackerangriff

Nach der Hacker Attacke auf den Feuerwehrausstatter Rosenbauer mit Sitz in Leonding (Bezirk Linz-Land) laufen jetzt die Bemühungen, die IT-Systeme bald wieder hochzufahren. Bei dem Cyber-Angriff vergangene Woche war die gesamte IT-Infrastruktur des Unternehmens lahmgelegt worden.

3. März 2023, 6.17 Uhr Teilen

Seit vergangenem Freitag arbeiten Fachleute der IT-Abteilung von Rosenbauer und externe Cyber-Security Experten auf Hochtouren, die internen Systeme wiederherzustellen. Das dürfte nun auch fast geschafft sein.

Betrieb nach wie vor eingeschränkt

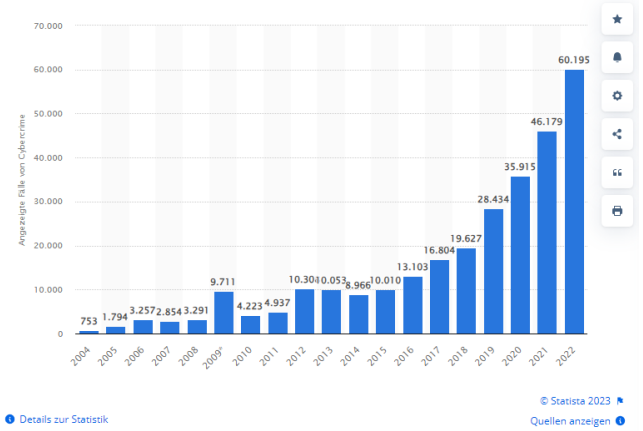
Anfang nächster Woche soll alles wieder hochgefahren werden. Die gesamte IT-Infrastruktur werde neu aufgesetzt, heißt es aus dem Unternehmen. Eine eigens eingerichtete Taskforce aus IT-Experten arbeitet rund um die Uhr im Unternehmen. Aus Sicherheitsgründen wurden alle Systeme vergangene Woche abgeschaltet. Der Betrieb läuft seither stark eingeschränkt weiter.

Krisen und Schadensfälle

Cyberangriffe in Österreich um 201% gestiegen laut KPMG Studie 2023 (KPMG Studie: Cybersecurity in Österreich 2023 - KPMG Austria)

Cyberangriff Varianten aus der Praxis:

- Phishing und Spear Phishing
- Investition in Kryptowährungen (Anlagebetrug)
- Einkaufs/Verkaufs-Betrug (Facebook, Instagram, Willhaben, Vinted, Tinder, SMS, Anrufe, etc.) mit Fake Profilen, Fake Shops und Love Scams
- Eltern/Kinder, Neffen Trick – verlorenes Handy, zu bezahlende Rechnungen
- Microsoft/Europol Mitarbeiter – Remote Verbindung nach Installation von Anydesk, Teamviewer, etc.
- Impersonisierung (Amazon, DHL, Post, etc.)
- Apple Wallet
- Finanzamt Rückzahlung oder Forderung
- Gefälschte Rechnungen



Techniken der Angreifer

- Social Engineering
  - Aufbau von Stress, Zeitdruck, Fake Ereignisse, Phishing von Daten, etc.
- CEO Fraud
- Phishing URLs – Fake Domains mit 1:1 nachgebauten Seiten
  - Suchmaschinen Ads werden verwendet um auf Fake Domains umzuleiten
- Repackaged Applikationen, Screen Reading (Man in the Application)
- Trojaner, Malware (Man in the Middle)
- Cybercrime as a Service (DDoS, Malware, Ransomware, etc.)

Risiken und Auswirkungen

43% an Cyberangriffen zielen auf KMU, insbesondere in den Bereichen Einzelhandel, Versicherungen, Recht, Gesundheitswesen und Finanzwesen laut Avast (Was sind Angriffsflächen und wie verringert man sie? | Avast)

95% der Cybersicherheitslecks werden durch Fehleinschätzungen und Irrtümer verursacht laut Avast (Was sind Angriffsflächen und wie verringert man sie? | Avast)

- Unberechtigte Offenlegung sensibler und vertraulicher Informationen nach Extern
- Eindringen in die Unternehmenssphäre durch leicht überwindbare Sicherheitsbarrieren (physisch und technisch)
- Datenverlust und Offenlegung personenbezogener Daten durch Datenschutzpanne
- Nicht Verfügbarkeit von Geschäftsrelevanten Diensten

Handlungsempfehlungen (Sicherheitsmaßnahmen)

- Security Awareness Training
- Keine Offenlegung von Firmendaten durch Mitarbeiter
  - Keine Weitergabe sensibler oder interner Informationen, auch nicht in sozialen Medien
  - Keine sensiblen Telefonate oder Online Meetings in der Öffentlichkeit
  - Keine Eingabe von Benutzername und/oder Passwort in unbekannten Web Formularen

- Bei Verdacht oder bestätigten Sicherheitsvorfall Kontaktaufnahme mit IT-Security bzw. Strafverfolgungsbehörde
  - Keine Offenlegung von Details im Falle eines Sicherheitsvorfalls

Handlungsempfehlungen (Sicherheitsmaßnahmen)

- Phishing und Fraud Erkennung Software inkl. Anomalie Erkennung und Verhaltensanalyse
- Phishing URL Takedown Service
- Cyberversicherung
- Incident Response Retainer Service
- MDR & SIEM/SOC – Erkennen und stoppen von Bedrohungen innerhalb kürzester Zeit
- Absicherung der Remotezugänge und Lieferantenzugänge
- Security gemanagt Endgeräte und Mobilgeräte
- Vertraglich vereinbarte Lieferantenaudits

Handlungsempfehlungen (Sicherheitsmaßnahmen)

- Implementierung einer Data Loss Prevention (DLP) Lösung gegen den absichtlichen und unabsichtlichen Datenverlust
- Erstellung von verpflichtenden Unternehmensrichtlinien zur Klassifizierung von Daten (Labeling) und den Umgang mit Unternehmensdaten
- Einsatz von Multi-Faktor-Authentifizierung (MFA) wo immer es möglich ist
- Einbeziehung aller relevanten Stakeholder
- Vorgaben betreffend sicherer Software Entwicklung, z.B. Leitfaden BSI
- Orientierung an Standards, z.B. ISO 27001, IEC 62443
- Zertifizierungen, z.B. ISO 27001, ISAE 3402, SOC 2 Type 2, etc.
- Einhaltung der gesetzlichen Anforderungen, z.B. DORA, NIS 2.0
- Einhaltung regulatorischer Anforderungen der Aufsicht, z.B. EZB, BaFin, FMA, etc.

Handlungsempfehlungen (Sicherheitsmaßnahmen)

- Notfallpläne (Business Continuity Plans)
- Runbooks, z.B. Ransomware, DDoS, APT
- Cybercrime Resilience Übung – Notfallübungen
- Technische und organisatorische Maßnahmen (TOMs) für Informationssicherheit und Datenschutz
- Sicherheitsstrategie und Sicherheitsanforderungen / Mindeststandards an Dienste und Lieferanten

Fachkräftemangel

- Der IT-Fachkräftemangel macht 38% der Betriebe zu schaffen laut Deloitte (Cyberangriffe in Österreich werden immer professioneller | DiePresse.com)
- Erweiterung des Angebots von Studiengängen an Universitäten und FHs
- Enge Zusammenarbeit zwischen Wirtschaft und Bildungssektor notwendig
- Projektarbeiten, Bachelor und Masterarbeiten von StudentInnen für Unternehmen
- Spannende Vorträge aus der Praxis von Experten an Universitäten und FHs
- Erweiterung des Angebots Duales Studium – Praxis und Theorie
- Präsenz der Unternehmen bei IT-Security Veranstaltungen, Konferenzen und Messen

Weiterführende Literatur

- Internet Organised Crime Threat Assessment (IOCTA) Europol Report 2023 (https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf)
- Crowdstrike 2023 Global Threat Report (https://www.crowdstrike.com/global-threat-report/#)
- 2023 Threat Detection Report Red Canary – Techniques, Trends and Takeaways (2023 Red Canary Threat Detection Report)
- BSI: Schutz vor Ransomware – Präventive Maßnahmen zur Absicherung vor Krypto-Trojanern (Schutz vor Ransomware (allianz-fuer-cybersicherheit.de))
- TeleTrusT – Handreichung zum „Stand der Technik“ in der IT-Sicherheit (teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf)
- Myra Security, Whitepaper DORA: Harmonisierte Regulatorik für mehr Cybersicherheit im EU-Finanzsektor erhöht Compliance Hürden (DORA: Regulatorik für Cybersicherheit im Finanzsektor (myrasecurity.com))
- WKO (Mag. Verena Becker, BSc), Die neue Cybersicherheits-Richtlinie NIS2 (PowerPoint-Präsentation (wko.at))

Vielen Dank für Ihre Aufmerksamkeit!