



Tag der Landtechnik

Cyber Safety - Mehr Sicherheit im digitalen KMU Alltag



Agenda

- Cyber Bedrohungen
- Lösungsszenarien
 - Prävention
 - Erkennung
 - Reaktion
 - Awareness im Unternehmen

TRITON Malware: Angriff auf ein Kraftwerk in Saudi Arabien

Es war ein Angriff einer neuen Dimension: Ende 2017 attackierten Hacker ein Kraftwerk in Saudi-Arabien. Ziel der Cyberattacke war es vermutlich, die Anlage zu zerstören. Die Angreifer nahmen dabei Tote und Verletzte in Kauf. Der außergewöhnlich anspruchsvolle Angriff fiel nur auf, weil die Malware versehentlich eine Sicherheitsabschaltung des Kraftwerks auslöste.

Der Angriff sollte nicht nur dem Staat am Persischen Golf zu denken geben, sondern auch in Deutschland für Alarmbereitschaft sorgen: Denn die Attacke lief über ein Sicherheitssystem, das auch in Hunderten deutschen Industrieanlagen im Einsatz ist.

Als konkretes Angriffsziel wählten die Hacker in Saudi-Arabien einen zehn Jahre alten Controller im sogenannten Triconex Safety Instrumented System (SIS) des Herstellers Schneider Electric. Die Einheit kommt weltweit in Öl- und Gaskraftwerken, aber auch in Atomanlagen zum Einsatz. Sie dient dazu, in kritischen Situationen vorher festgelegte Routinen auszuführen.

Überhitzt beispielsweise ein Kraftwerk, sorgt das Modul für das automatische Herunterfahren der Anlage oder reguliert den Druck und die Temperatur. Schneider gibt an, weltweit über 13.000 der Sicherheitssysteme verkauft zu haben.

Spiegel Online, 6. April 2018



Merkel und der „fancy bear“

Gut möglich, dass im Wahlkampf demnächst E-Mails der Kanzlerin auftauchen. Oder vertrauliche Dokumente aus dem Bundestag. Denn vor zwei Jahren spionierten Hacker wochenlang das Computernetzwerk des Parlaments aus.

Die Zeit, 10. Mai 2017

Hacker-Gruppe veröffentlicht medizinische Daten

Der Hacker-Skandal um die russische Gruppe Fancy Bear hat Deutschland erreicht. Im Hintergrund deutet sich eine Annäherung zwischen WADA und Russland an.

Von 25 Athleten veröffentlichten die Cyber-Piraten in der Nacht zum Donnerstag medizinische Daten, darunter Leichtathletik-Stars sowie von drei deutschen Schwimmern. Spektakuläres war wieder nicht dabei, die Daten offenbaren keine illegalen Aktivitäten.

TZ München, 15. September 2016

APT28 - das sind die Hacker hinter dem Angriff auf das Bundesnetzwerk

Das Hacker-Kollektiv ATP28 oder „fancy bear“ ist in der Szene schon lange berüchtigt. Die Abkürzung steht für "Advanced Persistent Threat", ein Begriff, der sich am besten mit "Fortgeschrittene und anhaltende Bedrohung" übersetzen lässt.

Ihnen wird etwa der Angriff auf den Bundestag 2015 zugeschrieben, sie attackierten europäische Rüstungskonzerne, Webprovider und Energieunternehmen. Auch der Hacker Guccifer 2.0, der vor der Wahl die Server der US-Demokraten infiltrierte, wird der Gruppe zugerechnet, weil er Teile ihrer Software benutzte.

Spiegel Online, 28. Februar 2018



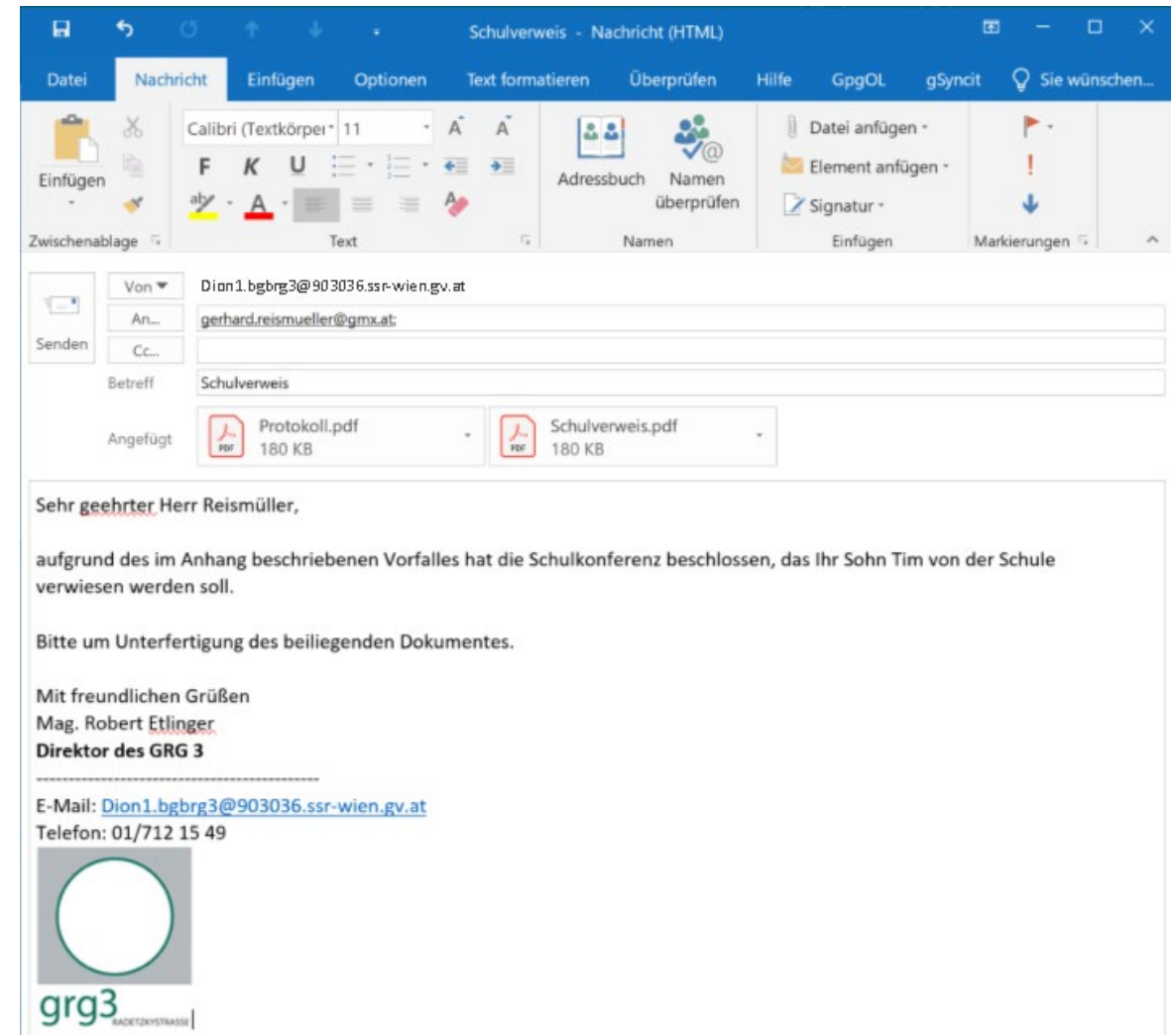
APT28
Fancy Bear

Ukraine: Hackerangriff verursachte Blackout

Offenbar haben es Hacker geschafft, einen Stromausfall zu verursachen. Am 23. Dezember war in einem großen Teil des Oblasts Ivano-Frankivsk mitsamt der Hauptstadt in der Westukraine für mehrere Stunden der Strom ausgefallen. Nach einem lokalen Medium, das am 24. darüber berichtete, sei dafür ein Computervirus verantwortlich gewesen. Hacker seien danach in das Steuerungssystem des Energiekonzerns Prykarpattiaoblenergo eingedrungen.

Nach der Sicherheitsfirma ESET sind nicht nur bei Prykarpattiaoblenergo, sondern auch bei zwei weiteren Energieunternehmen Viren gefunden worden. BlackEnergy wird als Anhang von Mails geschickt und führt dann, wenn angeklickt, "Trojan Win32 / Killdisk" aus. Das sei auch bereits in der Ukraine während der lokalen Wahlen im November gegen ukrainische Medien beobachtet worden, allerdings sei es da um Spionage gegangen. Hier wurde Killdisk erstmals entdeckt. Bei dem aktuellen Angriff wurden nicht nur Dateien gelöscht, sondern es gab auch die Funktion, das Booten zu verhindern, um so Industrieanlagen besser und nachhaltiger lahmlegen zu können.

Telepolis, 5. Jänner 2016



Stillstand nach Cyberangriff auf Aufzugsbaukomponenten-Firma Wittur

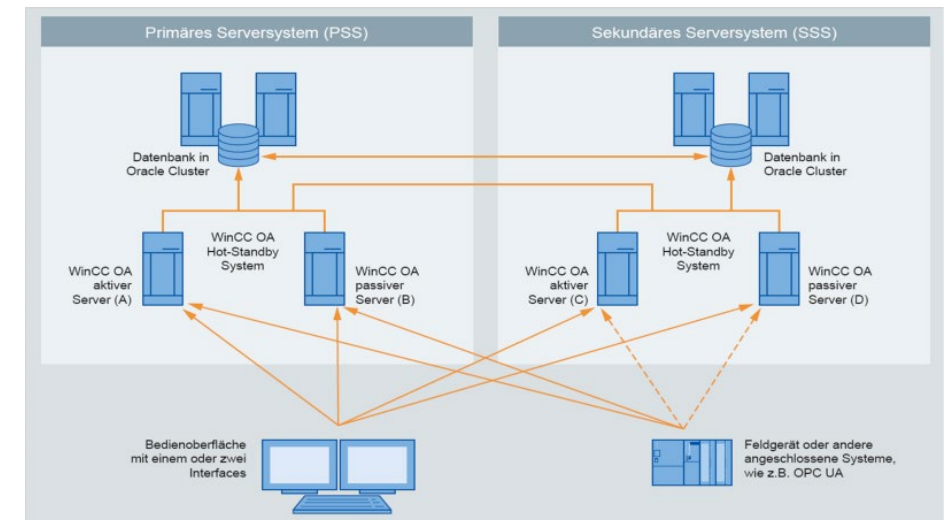
Weltweit steht die Fertigung in der deutschen Firma Wittur still. Nach einem Angriff wurden die Server heruntergefahren. Externe Spezialisten wurden zur Behebung des Problems hinzugezogen.

Die deutsche Aufzugskomponenten-Firma Wittur ist Opfer eines Cyberangriffs geworden. Wie der ORF Niederösterreich berichtete, stand am Mittwoch die Fertigung in allen Werken still. Auch die Niederlassung in Scheibbs, in der 550 Mitarbeiter beschäftigt sind, ist demnach betroffen. In den nächsten Tagen soll die Produktion wieder aufgenommen werden.

Am Samstagabend soll die interne Überwachung angeschlagen haben, heißt es in dem Online-Bericht. Die Wittur-Gruppe mit Sitz in Wiedenzhausen bei München bestätigte dem ORF, dass es einen "Cyber Security Event" gegeben habe und diverse Teile des IT-Systems betroffen seien. 100 Server an 16 Standorten seien wegen des Angriffs heruntergefahren worden. Michael Bach, Geschäftsführer der Wittur Austria GmbH erklärte, dass ab "Freitag, 14 Uhr" wieder alle Server laufen sollten.

Die Presse, 13. Februar 2019

Hochredundante Systeme:
Verfügbarkeit versus Segmentierung
Infiziertes Backup



380 000 Kreditkarten-Daten bei British Airways gestohlen

Bei Buchungen über die Website und die App von British Airways sind nach Angaben der Fluggesellschaft die Daten von etwa 380 000 Kreditkarten gestohlen worden. Betroffen seien persönliche und finanzielle Details, nicht aber Pass- und Reisedaten, teilte die Airline am Donnerstagabend in London mit. Demnach konnten die Informationen über einen Zeitraum von rund zwei Wochen – vom Abend des 21. August bis zum Abend des 5. September abgegriffen werden. «British Airways ist im Kontakt mit betroffenen Kunden», so die Airline. Die Behörden seien informiert worden.



Mindestens 500 Millionen Yahoo-Kunden bestohlen

Beim Internetkonzern Yahoo sind bei einem Hacker-Angriff im Jahr 2014 Daten von mindestens 500 Millionen Nutzern gestohlen worden. Es gehe um Namen, E-Mail-Adressen, Telefonnummern, Geburtstermine und verschlüsselte Passwörter, teilte das amerikanische Unternehmen am Donnerstag mit. Es seien weder Passwörter im Klartext noch Kreditkarten- und Bankkonto-Informationen entwendet worden.



Sony räumt weiteren Diebstahl von Kundendaten ein

Beim japanischen Elektronikkonzern Sony ist es offenbar zu einem weiteren Diebstahl von Kundendaten gekommen. Es seien möglicherweise Informationen von knapp 25 Millionen Kunden des Spiele-Netzwerks Sony Online Entertainment gestohlen worden, teilte Sony mit. Darunter seien 12'700 Nummern von Kreditkarten.

Neue Züricher Zeitung, 2011 - 2018



Lösungsszenarien



Cyber Security in Österreich

Key Findings 2018

Tatort Internet

Österreichs Unternehmen im Visier

60%

der Angriffe zielen auf die „Schwachstelle Mensch“

61%

der Unternehmen waren Opfer einer Cyberattacke

73%

fühlen sich in Cyber Security-Belangen wohl

91%

haben ihr Verständnis für Cyberrisiken verbessert

52%

prognostizieren einen Anstieg des Cyber Security-Budgets

45%

melden cyberkriminelle Vorfälle nicht

Zwischen Angriff und Verteidigung

Aktion & Reaktion der Unternehmen

26%

geben an, dass Digital Labor bereits jetzt eine wichtige Rolle spielt

32%

erfahren Cyber Security-Herausforderungen durch Künstliche Intelligenz

Wirksame Verteidigung

Künstliche Intelligenz bietet innovative Möglichkeiten

Neue Spielregeln für Sicherheit

Das Internet ist kein rechtsfreier Raum

15%

sehen in der Löschung der Daten das größte Problem der DSGVO-Umsetzung

74%

erwarten eine Zunahme der Kundenanfragen zum Datenschutz

Mit Strategie zum Erfolg

Cyber Security als Chefsache

45%

führen eine Messung der Cyber Security-Risiken mittels Kennzahlen durch

79%

diskutieren Cyber Security-Themen auf oberster Unternehmensebene

67%

der Unternehmen beklagen einen Mangel an Cyber Security-Experten

49%

glauben, dass die Cloud-Nutzung den Infrastrukturaufwand verringert

Auf neuen Wegen

Die Zukunft der Cyber Security in Unternehmen

* Im März und April 2018 wurden 269 österreichische Unternehmen von KPMG befragt, wie sie den Herausforderungen durch Cyberkriminalität begegnen und welche Cyber Security-Maßnahmen sie treffen. Die Umfrage wurde in Kooperation mit dem Sicherheitsforum des KSO (Kuratorium Sicheres Österreich) durchgeführt und kann per E-Mail an publikationen@kpmg.at angefordert werden.

Prävention *organisatorisch*:

- Implementierung von Methoden/Systemen
 - IKS, ISO27000, ISMS, ITIL, etc.
 - **best practise** versus **Zertifizierung**
 - Richtlinien für Updates, Passworte, etc.
 - Zugang (auch **physisch**), USB, etc.
- **Notfallplanung**
 - Alarmierung, Eskalation
 - Technische Maßnahmen
 - Verständigungen (Mitarbeiter, Kunden, Behörden, Experten, etc.)
- **Tests**: Penetration (technisch und sozial), Notfallübungen
- Cybersicherheit muss ein Thema der **Chefetage** sein und von dort aus gesteuert werden



Prävention *sozial*:

- **Awareness** !!!!
 - Schulungen, Trainings
 - Intranet, Newsletter
- **Notfallplanung**
 - Alarmierung, Eskalation
- **Tests**: Penetration (technisch und sozial), Notfallübungen
- Cybersicherheit muss ein Thema der **Chefetage** sein und von dort aus gesteuert werden



Erkennung:

- Monitoring
- Logging
- Penetrationtests

Kosten / Expertise / Ressourcen



Outsourcing:

Cloud

versus

ASP

versus

Home



Reaktion:

➤ **Bewältigung** von Notfällen und Krisen

➤ **Planen**

➤ **Testen**

➤ **Trainieren**

