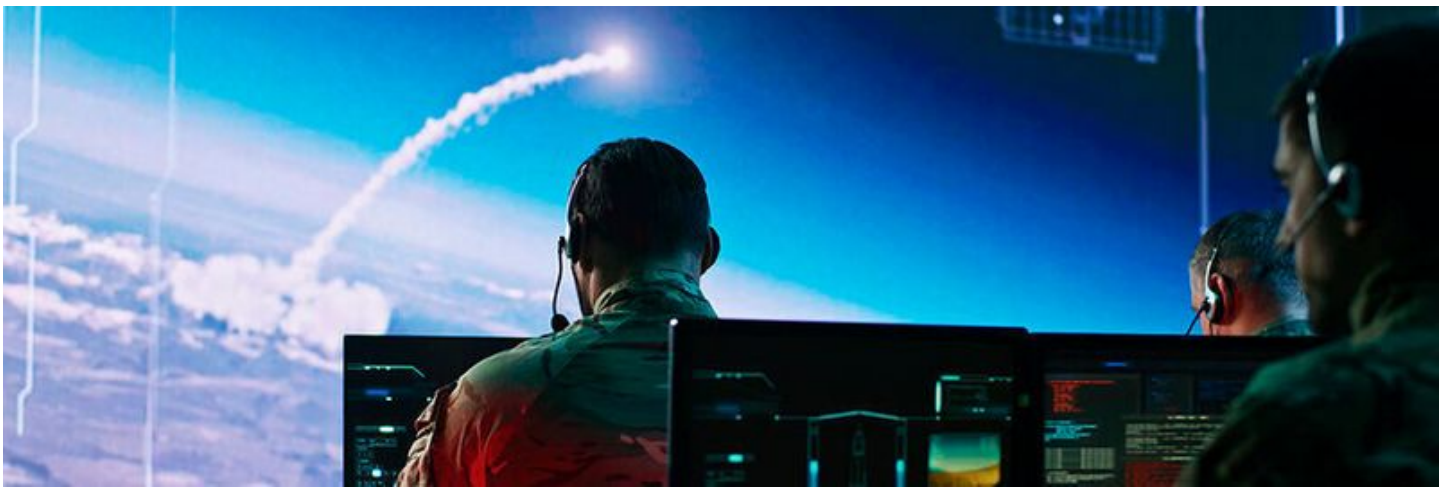
Der Cyber-GAU

Notfallpläne für die Cyberapokalypse

19.11.2021 | Autor / Redakteur: Anna Kobylinska, Filipe Martins / Peter Schmitz

Die digitaltransformierte Wirtschaft ist zutiefst cyberverwundbar. Sie scheint stets nur knapp eine Haaresbreite weg vom nächsten GAU, ein Zero-day-Exploit abseits der Totalkatastrophe, in die nächste Panne zu schlittern. Viele Sicherheitsforscher sehen den Status-Quo als kollektive Leichtsinnigkeit an. Sie warnen vor dem drohenden Gespenst der Cyberapokalypse.



Cyberkriminelle bedrohen mit ihren Aktionen immer öfter das tägliche Leben und sogar die Gesundheit vieler Millionen Menschen. Es wird Zeit, dass die Gemeinschaft sich Notfallpläne überlegt.
(© Framestock - stock.adobe.com)

Seit Anbruch der Pandemie mehren sich Cyber-Attacken gegen die Unternehmens-IT über den Angriffsvektor <https://www.security-insider.de/was-ist-ein-angriffsvektor-a-1071184/> Home-Office, über – und gegen – cyberphysische Systeme der Industrie 4.0, IoT-Endpunkte der Logistik und andere potenzielle Einfallstore. Selbst die eigenen Versorgungsketten der betroffenen Firmen stellen eine Gefahr dar (siehe auch den Bericht „IoT unter Beschuss. Risiko: Supply-Chain-Attacken“ <https://www.security-insider.de/risiko-supply-chain-attacken-a-920880/>). Phishing <https://www.security-insider.de/was-ist-phishing-a-591842/> läuft auf hohen Touren. Ransomware <https://www.security-insider.de/was-ist-ransomware-a-781385/> -Angreifer kassieren weiter ungestraft ab. Ist das jetzt die „neue Normalität“ oder wie? Einfach Augen zu und durch? Wohl kaum.

Die Wirtschaft und Gesellschaft sind in einem digitalen Gewebe ineinander verflochten, „mit heißer Nadel gestrickt“ und cyberverwundbarer denn je. Digitale Zahlungssysteme und Versorgungsketten umspannen die Welt. Robotik dominiert bereits die Fertigung. Autonome Fahrzeuge sind schon dabei, auch noch die Logistik zu erobern. Für viele Unternehmen ist die digitale Revolution kaum noch in den Griff zu bekommen. Die spektakuläre Solar-Winds-Attacke stellte dies ja auch Ende des vergangenen Jahres ausdrücklich unter Beweis. Es hätte noch viel schlimmer kommen können. Es scheint ja nur eine Frage der Zeit, bis etwas in richtig großem Umfang auch wirklich schiefgeht.

Wie ein Kartenhaus

Die „Cloudifizierung“ der Unternehmens-IT eilt den Cyber-Fähigkeiten der betreffenden Organisationen voraus, warnen Analysten von Check Point Research (2021 Cyber Security Report). Die Sicherheit der öffentlichen Cloud stellt für drei von vier Unternehmen (75 Prozent) immer noch ein großes Problem dar. Im Durchschnitt alle 10 Sekunden fällt irgendwo auf der Welt ein neues Unternehmen einer Ransomware-Attacke zum Opfer. Doch die Folgen sind nicht in 10 Sekunden von der Hand zu weisen.

Travelex, ein in London ansässiges Devisenhandelsunternehmen, musste es auf die harte Tour lernen. Eine Ransomware-Bande, gewappnet mit der Ransomware-as-a-Service-Malware <https://www.security-insider.de/was-ist-malware-a-578417/> Sodinokibi (alias REvil) wollte zum Silvesterabend 2019 6 Millionen Dollar einkassieren. Als sich das Unternehmen weigerte, das geforderte Lösegeld im Tausch für die Krypto-Schlüssel zu seinen Datenbeständen zu zahlen, drohten die Angreifer mit Vergeltung: der Veröffentlichung – statt bloßer Vernichtung – von 5 GB an persönlich identifizierbaren Kundendaten. Travelex hat das Lösegeld auf 2,3 Millionen heruntergehandelt und dann auch prompt gezahlt. Daraufhin musste das Unternehmen den Betrieb für mehrere Wochen einstellen, um die eigene IT zu entseuchen und sich von dem Desaster zu erholen.

Und das war „nur“ ein Devisenhändler, und zwar einer von vielen. Für die betroffenen Kunden hat es ja gereicht, einfach mal zum nächsten Geldwechselautomaten zu laufen, Problem gelöst.

Doch was passiert, wenn eine solche Panne mal das Stromnetz trifft? Wenn die Netzfrequenz für Millionen von Menschen zusammenbricht? Wenn alle digitalen Infrastrukturen, von der Telekommunikation bis hin zu Zahlungssystemen, wie ein Kartenhaus in sich zusammenbrechen?

Ungeachtet der Jahreszeit bekäme die moderne Gesellschaft einen Vorgeschmack die Cyberapokalypse aus einem Hollywood-Kassenschlager. Wird schon nicht passieren, oder wie?

Ohne Strom gibt es kein Internet, Sie könnten jetzt also schon mal nicht mehr weiterlesen. Mobil vielleicht? Ja, aber nur wenn die Mobilfunkmasten mitspielen und andere kritische Elemente der Infrastruktur nicht vor lauter Überlastung „durchbrennen".

Die meisten Rechenzentren könnten sich jedenfalls so um die 12 Stunden lange per Dieselgenerator mit Ach und Krach im Betrieb halten. Das reicht mit Glück, um die Arbeitslasten und Daten woandershin zu schieben, wenn das Woanders selbst Energie hat. Selbst jene Datencenter, die für den Betrieb kritischer Infrastrukturen <https://www.security-insider.de/was-ist-kritis-a-1021718/> (KRITIS) erforderlich sind, würden nicht einmal eine Woche durchhalten.

Könnten denn nicht zumindest erneuerbare Energiequellen wie Wind und Photovoltaik einspringen? Die Einwohner im energiereichsten U.S.-Bundesstatt Texas hatten ja dieses Jahr eine Probe aufs Exempel gemacht.

Windturbinen vom Netz, Tankstellen dicht

Nachdem im Februar ein Schneesturm auf Texas, den energiereichsten U.S.-Bundesstaat, einschlug, kamen die Windkraftanlagen zum Stillstand, weil die Windturbinen einfroren. Erdgas- und Kohlebefeuerte Kraftwerke konnten nicht schnell genug anspringen. Die Netzfrequenz brach stellenweise zusammen und kaskadierte zu Stromausfällen (den sogenannten „rolling blackouts") durch. Diese waren übrigens beabsichtigt, orchestriert sogar.

Denn das texanische Stromnetz sei nur wenige Sekunden (nicht Stunden!) davon entfernt gewesen, einen „katastrophalen Schaden" zu nehmen und unzählige Energieverbraucher für mehrere Monate (nicht Wochen!) völlig „stromlos" hängen zu lassen, enthüllte im Nachhinein ERCOT (Electric Reliability Council of Texas), die zuständige Behörde.

Unter den Stromverbrauchern, wie sich das so schön nennt, gibt es, zumindest in Texas, auch das eine oder andere Kernkraftwerk, das sich ohne Stromversorgung ähnlich wie Fukushima mit einer Kernschmelze verabschiedet hätte. Die Totalkatastrophe konnte knapp verhindert werden, doch das ist gerade ja schwacher Trost.

Denn wenn es schon ein Schneesturm schafft, durch den Zusammenbruch der Netzfrequenz einen permanenten Schaden an den cyberphysischen Infrastrukturen der Energieversorgung anzurichten, kann es in einem vollständig digitalisierten, „smarten“ Stromnetz eine Bande von Hackern erst recht. Im Übrigen: In einem Gleichstromnetz würde die Gefahr erst gar nicht entstehen. Mittlerweile wäre ein solches Stromnetz auch machbar, zum Beispiel mit der Technik von Siemens. Nur es fehlt offenbar der Wille. PV-Anlagen und Windturbinen, die ihre Leistung an ein Wechselstromnetz abgeben, können die Netzfrequenz im Alleingang nicht halten.

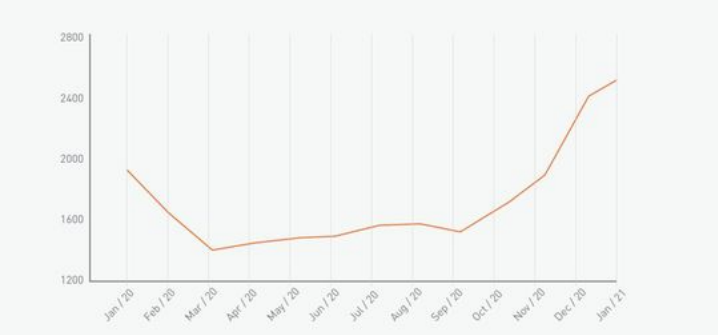
Tanzen auf dem Vulkan

Ein Zusammenbruch der Energieversorgung braucht nicht erst noch ein Atomkraftwerk, um den Tagesablauf von Millionen von Menschen auf unbestimmte Zeit zu destabilisieren. Das Auto würde vielleicht noch anspringen, aber es würde sich schon ganz sicher nicht mehr aufladen oder betanken lassen.

Die Lebensmittelketten hätten als erste die Türen verriegelt, denn elektronische Kassensysteme laufen ja nicht ohne Strom. Photovoltaik auf dem Gelände nützt nichts ohne massive Batteriespeicher; das Stromnetz verschlingt ja bereitwillig die Leistung – und gibt sie nicht wieder ab. (Das haben schon die Kalifornier ausprobiert, die ihre Photovoltaik-Leistung an das öffentliche Stromnetz verkaufen wollten.)

Inzwischen ist auch alles daheim drüber und drunter. Der Kühlschrank schmilzt, Induktionsplatte tot. Kein Online-Verkauf, kein Handel überhaupt. Mal scheuen, was die Nachbarn machen. (Hoffentlich sind die nett.) Mit Familie per Facetime plaudern geht auch nicht mehr. Ohne funktionsfähige Mobilfunkmasten entfällt das Telefonieren, selbst wenn das Kern-RZ noch mitspielt. Hilfe rufen geht also auch nicht. Nicht schlimm. Es würde eh niemand kommen.

Hacker <https://www.security-insider.de/was-ist-ein-hacker-a-596399/> und andere Cyber-Täter sollen ja bereits die COVID-19-Pandemie gekonnt ausgenutzt haben. Angriffe auf den Gesundheitssektor hätten die Ausmaße einer Epidemie eingenommen, jammern die Analysten von Check Point Research. Das Unternehmen meldete im Dezember des vergangenen Jahres einen Zuwachs von Cyberangriffen auf Krankenhäuser weltweit um 45 Prozent in einem Zeitfenster von nur zwei Monaten. Die Universität von Kalifornien zahlte eine Million Dollar an eine Ransomware-Bande, um die mit der Crimeware Netwalker zermuxten Forschungsdaten der medizinischen Fakultät zu COVID-19 entschlüsseln zu lassen.



Die Anzahl von monatlichen Cyberattacken im Gesundheitssektor (hier pro befragte Organisation) hat laut den Analysten von Check Point Software „die Ausmaße einer Epidemie" eingenommen.
(Bild: Check Point Software)

Cyber-Täter drohen Unternehmen zusätzlich zur Vernichtung von Daten (die sich aus einem Backup <https://www.security-insider.de/was-ist-backup-a-954035/> wiederherstellen ließen) auch noch mit dem Offenlegen von Geheimnissen, was dem Opfer vernichtende DSGVO-Strafen aufbürden kann. Jede zweite Ransomware-Attacke ab dem dritten Quartal des vergangenen Jahres hat diese zusätzliche Dimension, warnt Sicherheitsspezialistin Check Point Software in einem aktuellen Bericht.

Ein beliebtes Ziel von Cyber-Kriminellen sind Mobiltelefone. In 46 Prozent der Unternehmen hat mindestens ein Mitarbeiter schon mal eine schädliche mobile Anwendung heruntergeladen. Sicherheitstools auf Mobilgeräten sind immer noch eine Rarität.

Bewährte Techniken zum Schutz hochsensibler Zugriffe auf die Unternehmens-IT versagen. So konnten Täter im Pandemiejahr sogar Schutzvorkehrungen wie 2FA <https://www.security-insider.de/was-ist-eine-zwei-faktor-authentifizierung-2fa-a-631495/> -Authentifizierung mit Vishing <https://www.security-insider.de/was-ist-ein-vishing-a-991470/ > (Voice-Phishing) wiederholt aushebeln, zum Beispiel durch das Social Engineering von Zugangstoken über gefälschte Support-Hotlines. Unmöglich? In Juli des vergangenen Jahres haben sich einige Mitarbeiter von Twitter auf eine solche Vishing-Kampagne eingelassen und gewährten den Angreifern Zugang zu internen Tools, die ihnen wiederum erlaubten, einige Promi-Accounts <https://www.security-insider.de/was-ist-ein-account-a-799384/> wie jenes von dem damaligen U.S.-Präsidentschaftskandidaten Joe Biden und Amazon CEO Jeff Bezos zu übernehmen. Ein paar Stunden später waren die Täter mit über hunderttausend Dollar an Lösegeld auf und davon.

Im ganzen vergangenen Jahr sollen laut der Cybersicherheitsfirma Tenable infolge von rund 730 separat gemeldeten Verletzungen über 22 Milliarden (Engl. 22 Billion) Datensätze weltweit in die falschen Hände geraten sein (2020 Threat Landscape Retrospective Report). IDC klassifiziert Tenable als den weltweiten Marktführer im Markt für Lösungen zum Absichern von Mobilgeräten gegen Cyberverwundbarkeiten.

Schätzungen von Check Point Software zufolge lauern auf ihre Opfer jeden Tag zehn Tausend bösartige Downloads und rund zehn Mal so viele (100.000) bösartige Websites.

Fazit

Nach der Krise ist vor der Krise. Es wäre vielleicht langsam an der Zeit, sich für die digitaltransformierte Realität den einen oder anderen Fallback zu überlegen und auch mal zu implementieren.

Über die Autoren: Anna Kobylinska und Filipe Pereira Martins arbeiten für McKinley Denali Inc. <https://www.mckinley-denali.com/corporate/> (USA).

(ID:47802667)

KOMMENTARE