Assecuranzmakler GmbH

Cyber-Risiken

Inhaltsverzeichnis

Freitag, 17. Mai 2024

Deepfakes in Video-Konferenz

Geklonter Finanzvorstand ordnet Millionenbetrug an

Ein Mitarbeiter des britischen Ingenieurkonzerns Arup denkt, in einem Video-Call mit dem Finanzvorstand und anderen Kollegen zu sprechen. Danach überweist er Millionen auf mehrere Konten. Doch die anderen Teilnehmer waren durch Künstliche Intelligenz erschaffene Fälschungen.

Der britische Ingenieurkonzern Arup hat umgerechnet 23 Millionen Euro an Betrüger überwiesen, weil ein Angestellter durch Deepfakes in einer Video-Konferenz getäuscht wurde. „Wir können bestätigen, dass gefälschte Stimmen und Bilder verwendet wurden", teilte das Unternehmen der „Financial Times" mit. Einzelheiten nannte es nicht, da der Vorfall noch untersucht werde. Deepfakes sind gefälschte Videos, die mithilfe Künstlicher Intelligenz erstellt werden und extrem realistisch aussehen.

Getäuscht wurde ein Mitarbeiter der weltweit tätigen Firma in Hongkong. Die dortige Polizei hatte – ohne den Namen der betroffenen Firma zu nennen – mitgeteilt, dass ein Angestellter bei einem ausgeklügelten Betrug dazu gebracht wurde, an einer Video-Konferenz teilzunehmen. Er habe angenommen, dass es sich bei den anderen Teilnehmern um den Finanzchef des Unternehmens und weitere Mitarbeiter handele. Doch diese waren durch KI erschaffene Fakes.

Nach Angaben der Polizei hatte der Mann zunächst zwar vermutet, er habe eine angeblich von der britischen Niederlassung des Unternehmens verschickte Phishing-E-Mail erhalten – denn darin sei von einer „geheimen Transaktion" die Rede gewesen. Doch nach der Video-Konferenz verschwanden seine Zweifel. Denn die Deepfake-Schöpfungen sahen aus und sprachen wie die realen Kollegen, die er kannte.

Daraufhin überwies er 200 Millionen Hongkong-Dollar in 15 Transaktionen auf verschiedene Konten. Weil ihm das später doch wieder merkwürdig vorkam, fragte er in der Zentrale in London nach. Damit sei der Betrug aufgeflogen, so die Polizei.

Arup ist ein bekannter Ingenieurkonzern. Die Briten errichteten unter anderem die Oper in Sydney und das „Vogelnest"-Stadion in Peking. Weltweit beschäftigt das Unternehmen rund 18.000 Menschen und erwirtschaftete im vergangenen Jahr einen Umsatz von umgerechnet 2,3 Milliarden Euro.

Dienstag, 14. Mai 2024

Der Sport-Tag

Böse Überraschung am Eingang: Fans haben Ärger wegen WM-Tickets

Bei der Eishockey-WM in Tschechien sind viele Fans auf gefälschte oder wiederholt verkaufte Tickets hereingefallen.

In den ersten vier Tagen des Turniers habe man rund 300 derartige Fälle registriert, teilte die tschechische Polizei am Dienstag auf der Plattform X (vormals Twitter) mit. Der Gesamtschaden belaufe sich auf etwa 690.000 Kronen, umgerechnet rund 27.800 Euro.

Die Betrugsopfer bemerken den Schwindel demnach in der Regel erst, wenn das Drehkreuz am Stadioneingang den QR-Code auf ihrem Ticket nicht akzeptiert und eine Fehlermeldung erscheint. Am Reklamationsschalter erhalten die Betroffenen dann eine Bestätigung, mit der sie bei der Polizei Anzeige erstatten können.

An beiden Austragungsorten in Ostrava und Prag sind die Ordnungshüter unter anderem mit Experten für Cyberkriminalität vor Ort. Denn oft wurden die rechtswidrig weiterverkauften oder gefälschten Tickets auf Kleinanzeigen- und Wiederverkaufsplattformen im Internet erworben – nicht selten zu überhöhten Preisen.

Montag, 13. Mai 2024

BKA-Lagebild

Erneut steigende Tendenz bei Cyberangriffen 2023

Die Gefahren durch Cyberangriffe sind nach Einschätzung des Bundeskriminalamtes (BKA) im zurückliegenden Jahr weiter gestiegen. Dies geht aus dem jüngsten „Bundeslagebild Cybercrime“ hervor, das vorgestellt wurde. „Die polizeiliche Datenbasis, aber auch die Feststellungen einzelner IT-Security-Dienstleister zeigen für 2023 eine erneut steigende Tendenz bei Cyberangriffen sowohl in quantitativer als auch in qualitativer Hinsicht“, heißt es in dem Bericht.

Verantwortlich für diese Entwicklung seien insbesondere Fälle, die zwar Schäden in Deutschland verursachen, aber bei denen der Aufenthaltsort des Täters im Ausland liegt oder unbekannt ist. Die erfassten Cybercrimedelikte bei Auslandstaten stiegen laut Bundeslagebild 2023 im Vergleich zum Vorjahr um rund 28 Prozent. Mit Blick auf das Inland verzeichnete die Polizeiliche Kriminalstatistik für den gleichen Zeitraum mit minus 1,8 Prozent einen leichten Rückgang an Cyberstraftaten.

Zu den schwerwiegendsten Bedrohungen zählten nach wie vor Ransomware-Angriffe, bei denen Kriminelle die Daten von Unternehmen oder auch der öffentlichen Verwaltung verschlüsseln und ein Lösegeld für die Entschlüsselung fordern. Bundesweit haben 2023 mehr als 800 Unternehmen und Institutionen Ransomware-Fälle angezeigt, wie es im Bundeslagebild heißt.

Durch Cybercrime sind 2023 erneut hohe Schadenssummen verursacht worden, wie das BKA erklärte und auf Zahlen des Digitalverbandes Bitkom verwies. Demnach summierten sich die Gesamtschäden von analogem und digitalem Diebstahl, Industriespionage oder Sabotage für Unternehmen in Deutschland auf 205,9 Milliarden Euro. Von diesen Gesamtschäden führt Bitkom den Angaben zufolge fast drei Viertel auf Cyberattacken zurück.

Die explizit ausgewiesenen Schäden durch Erpressung mit gestohlenen oder verschlüsselten Daten belaufen sich auf 16,1 Milliarden Euro.

Freitag, 3. Mai 2024

Nach Cyber-Angriff auf SPD

Auswärtiges Amt bestellt russischen Diplomaten ein

Nach dem Abschluss der Ermittlungen ist sich die Bundesregierung sicher: Russland steckt „eindeutig" hinter dem Hacker-Angriff auf die SPD im Januar 2023. Nun zieht das Auswärtige Amt erste Konsequenzen – der amtierende Geschäftsträger der russischen Botschaft muss im Außenministerium vorstellig werden.

Das Auswärtige Amt hat als Reaktion auf einen russischen Cyber-Angriff auf die SPD im vergangenen Jahr den amtierenden Geschäftsträger der russischen Botschaft einbestellt. Der Geschäftsträger sei für 12 Uhr einbestellt, teilte ein Sprecher des deutschen Außenministeriums mit. Die Einbestellung sei ein diplomatisches Signal, „Moskau deutlich zu machen, dass wir dieses Vorgehen nicht akzeptieren, deutlich verurteilen und uns da auch Konsequenzen vorbehalten", ergänzte der Sprecher. Bei dem Geschäftsträger handelt es sich um Alexej Korljakow.

Vize-Regierungssprecher Wolfgang Büchner sagte, die Bundesregierung verurteile die wiederholten und inakzeptablen Cyber-Angriffe durch staatlich gesteuerte russische Akteure auf das Schärfste. Man fordere Russland erneut auf, derartige Handlungen zu unterlassen. „Deutschland ist entschlossen, gemeinsam mit seinen europäischen und internationalen Partnern solchen Cyber-Angriffen entgegenzutreten."

Die Aktionen der Cybergruppe APT28 könnten auf Grundlage belastbarer Informationen der deutschen Nachrichtendienste konkret dem russischen Militärgeheimdienst GRU zugeordnet werden, sagte Büchner. Die Kampagne richte sich auch gegen Regierungsstellen sowie Unternehmen aus den Bereichen Logistik, Rüstung, Luft- und Raumfahrt, IT-Dienstleistungen sowie Stiftungen und Verbände. „Sie war gegen Ziele in Deutschland und anderen europäischen Staaten sowie gegen Ziele in der Ukraine gerichtet", sagte er. APT28 sei auch verantwortlich für den Cyber-Angriff auf den Bundestag im Jahr 2015.

Das unverantwortliche Verhalten Russlands im Cyberraum stehe im Widerspruch zu internationalen Normen und verdiene insbesondere in einem Jahr, in dem in vielen Staaten Wahlen stattfinden, besondere Aufmerksamkeit, kritisierte Büchner. Cyber-Angriffe gegen politische Parteien, staatliche Institutionen und Unternehmen der kritischen Infrastruktur seien eine Bedrohung für Demokratie, nationale Sicherheit und freiheitliche Gesellschaft.

Die SPD hatte im Juni 2023 bekannt gegeben, dass E-Mail-Konten des SPD-Parteivorstands bereits im Januar Ziel eines Cyber-Angriffs geworden seien. Möglich geworden sei dies durch eine zum Zeitpunkt des Angriffs noch unbekannte Sicherheitslücke beim Softwarekonzern Microsoft, hieß es damals aus der SPD. „Es ist nicht auszuschließen, dass es zu einem Abfluss von Daten aus vereinzelten E-Mail-Postfächern kam", hieß es weiter.

Samstag, 20. April 2024

„Erschreckende Daten“

Cisco sieht Großteil der Industrie bei Cyberattacken gefährdet

Ob Continental oder die Kette Kind: Hackerangriffe werden immer mehr zur Bedrohung für Unternehmen. Einer Studie des Netzwerk-Ausrüsters Cisco zufolge ist Europas Industrie miserabel vorbereitet. Dabei ist die Eigenwahrnehmung der Betriebe oft besser als die Realität.

Die Industriebetriebe in Europa sind einer Studie zufolge nur unzureichend auf Hackerangriffe vorbereitet. Nur zwei Prozent der Unternehmen seien hier bestmöglich aufgestellt, bei 17 Prozent könne man immerhin von einem guten Schutz sprechen, heißt es in einer Studie des Netzwerk-Ausrüsters Cisco vor der am Montag beginnenden Hannover Messe. Bei mehr als 80 Prozent der Firmen bestehe dagegen Handlungsbedarf. Im Vergleich mit anderen Branchen liege die Industrie hier nur im unteren Mittelfeld.

Die besten Werte ermittelte Cisco für Technologie-Anbieter, wo immerhin 28 Prozent gut oder sehr gut vorbereitet seien, gefolgt von der Finanzbranche mit 23 Prozent. Auch im weltweiten Vergleich schneide Europas Industrie schlecht ab. In den USA seien 29 Prozent der Industriebetriebe gut oder sehr gut gegen Cyberattacken gerüstet, zehn Prozentpunkte mehr als in Europa. Am schlechtesten schnitten in Europa Bildungseinrichtungen und das Gesundheitswesen ab.

„Das sind erschreckende Daten“, sagte Christian Korff, Mitglied der Geschäftsführung bei Cisco in Deutschland. „Die europäische Industrie hat hier eindeutig Nachholbedarf, denn sie ist an vielen Stellen leicht verwundbar.“ Das könne zur ernsten Gefahr für den Standort werden. „Eine ausreichend gute Cyberabwehr kann heute über das Fortbestehen von Unternehmen entscheiden“, so der Manager, der auch Leiter der Bundesfachkommission „Künstliche Intelligenz und Wertschöpfung 4.0“ im Wirtschaftsrat der CDU ist.

Eigenwahrnehmung oft besser als die Realität

Für die Untersuchung hatte Cisco im Januar und Februar weltweit mehr als 8000 Führungskräfte aus Unternehmen befragt, davon knapp 2000 in Europa. 214 kamen aus der Industrie. Dabei habe sich auch gezeigt, dass sich die eigene Wahrnehmung der Unternehmen oft nicht mit der realen Gefahr decke. Fast 80 Prozent der befragten Ihnen in den nächsten ein bis zwei Jahren zu einer Unterbrechung des Betriebs wegen einer Cyberattacke kommen werde. „Das ist schon beeindruckend“, merkte Korff an. „Die Unternehmen fühlen sich relativ sicher, obwohl sie relativ schlecht vorbereitet sind.“

Vorfälle wie an der Uni Gießen, die nach einem Hackerangriff Ende 2020 monatelang offline war, zeigten, welche Gefahren drohten. „Wenn uns das im Herstellungsbereich passiert, dann brauchen wir uns um globale Lieferketten keine Gedanken zu machen. Dann steht hier die Produktion“, warnte Korff. Auch der Zulieferer Continental war im vergangenen Jahr Opfer einer Cyberattacke geworden, bei der Daten abgegriffen wurden. Beim Hörgerätehersteller Kind lag im Februar die zentrale Konzern-IT für mehrere Tage lahm, nachdem Hacker in das System eingedrungen waren.

Maschinen laufen oft noch auf Windows 95

Grund für das schlechte Abschneiden vieler Industriebetriebe sei vor allem die Langlebigkeit vieler Produktionsanlagen, sagte Korff. „Herstellungsprozesse werden ja schon seit 30 Jahren elektronisch

unterstützt. Da läuft als Betriebssystem zum Teil noch Windows 95 oder 98. Die sind natürlich nicht auf dem Stand der Technologie." Und sie seien auch nur schwer nachzurüsten. „Die alten Betriebssysteme und die vorhandenen Maschinen machen es extrem schwer, hier Sicherheitstechnologie einzubauen."

Etwas besser sehe es beim Thema Künstliche Intelligenz (KI) aus. 34 Prozent der Industrie seien hier gut oder sehr gut aufgestellt. Wirklich zufrieden könne man damit aber nicht sein, sagte Korff. Zwar hätten 64 Prozent der Betriebe eine KI-Strategie, doch nur 34 Prozent hätten auch die technische Infrastruktur, um KI wirklich einsetzen zu können. „Und wenn ich sehe, dass ein Drittel der Industrie-Unternehmen noch keine KI-Strategie haben, dann wird mir angst und bange", fügte Korff hinzu. Schließlich gehe es hier um die wohl wichtigste Schlüsseltechnologie der Zukunft.

„Die Fertigungsindustrie muss aufpassen, dass sie die beiden technologischen Megatrends Cybersicherheit und KI nicht verschläft – das gilt für Europa und Deutschland", warnte Korff. Sonst sei die Wettbewerbsfähigkeit in Gefahr. „Das ist existenziell für die deutsche und europäische Wirtschaft. Wenn wir nicht in der Lage sind, KI zu nutzen, uns aber gleichzeitig auch vor KI-Angriffen zu schützen, dann werden wir die nächste Dekade nicht überstehen."

©n-tv.de, vpe/dpa

Mittwoch, 27. März 2024

Initiative warnt vor Kriminellen

Schon jeder Zehnte erlebte Identitätsdiebstahl

Im Internet hinterlassen die meisten Nutzer eine Datenspur und ignorieren die Gefahren. Eine davon ist besonders perfide: Identitätsdiebstahl. Die Betroffenen bemerken den Schaden oft erst, wenn es zu spät ist. Eine Umfrage zeigt das Ausmaß des Problems.

Mehr als jeder zehnte Erwachsene in Deutschland (11 Prozent) ist bereits Opfer von Identitätsdiebstahl im Netz geworden. Das geht aus einer repräsentativen Umfrage des Meinungsforschungsinstituts YouGov im Auftrag der Initiative Sicher Handeln (ISH). hervor. Fast jeder fünfte Befragte (19 Prozent), der selbst bisher verschont geblieben ist, kennt aber einen oder gar mehrere Menschen, die Opfer wurden. Fünf Prozent haben beides erlebt, sind also selbst Opfer geworden und kennen weitere Opfer.

In der Online-Umfrage von YouGov wurden Anfang März 2058 Personen befragt. Die Ergebnisse wurden gewichtet und sind repräsentativ für die deutsche Bevölkerung ab 18 Jahren.

Identitätsdiebstahl sei eine besonders perfide Betrugsmasche, erklärte die Initiative. Kriminelle nutzten dabei Daten wie den Namen, das Geburtsdatum, die Anschrift oder Kreditkarten- oder Kontonummern ihrer Opfer, um sich mithilfe dieser Daten Nutzerkonten bei Online-Diensten anzulegen und auf fremde Kosten einzukaufen oder Verträge abzuschließen. „Die Opfer bekommen das meistens erst mit, wenn es zu spät ist und die Überweisungen auf dem Konto verbucht sind oder Rechnungen eintrudeln."

Vorsicht bei Post-Identverfahren

Aktuell nutzen viele Cyberkriminelle den angespannten Wohnungsmarkt aus. So werden etwa Wohnungssuchende mit einer gefälschten Anzeige dazu verleitet, ein Post-Identverfahren für eine Bewerbung für eine angebliche Wohnungsbesichtigung zu absolvieren. Oft merken die Betroffenen dabei nicht, dass sie mit den Angaben den Betrügern lediglich dabei helfen, in ihrem Namen ein Bankkonto zu eröffnen, das für kriminelle Zwecke verwendet werden soll, etwa für Geldwäsche.

„Obwohl die Gefahr steigt, nehmen viele das Thema offensichtlich noch immer auf die leichte Schulter", sagte eine Sprecherin der Initiative. Insbesondere die junge Generation agiere besonders sorglos. In der Umfrage sagte jeder dritte 18- bis 24-Jährige, für mehrere Nutzerkonten im Netz dasselbe Passwort zu verwenden. Im Schnitt handelt gerade einmal jeder Fünfte so. 16 Prozent der jungen Erwachsenen räumten ein, bereits eine Kopie ihres Personalausweises über das Internet mit einer fremden Person geteilt zu haben. Innerhalb der gesamten Stichprobe trifft das nur auf elf Prozent der Befragten zu.

Auch bei den Sicherheitsmaßnahmen handeln die älteren Befragten deutlich gewissenhafter als die jüngste Generation. 70 Prozent der Über-55-Jährigen sagen, dass sie regelmäßig ihre Kontoauszüge prüfen. Bei den 18- bis 24-Jährigen sind das lediglich 39 Prozent.

Sicher Handeln ist eine gemeinsame Initiative der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK), der Stiftung Deutsches Forum für Kriminalprävention (DFK), Deutschland sicher im Netze. V. (DsiN), RISK IDENT und Kleinanzeigen (ehemals eBay Kleinanzeigen), die 2023 ins Leben gerufen wurde.
9

Dienstag, 19. März 2024

Kult-Wagen nicht mehr zu kaufen

Viele beliebte Automodelle fallen neuen Cyber-Regeln zum Opfer

Durch neue Sicherheitsvorschriften, die im Sommer in Kraft treten, bieten Hersteller wie VW und Porsche diverse Automodelle in Deutschland nicht mehr an. Eine Überarbeitung der Fahrzeuge würde sich nicht lohnen, heißt es. Bestellungen können bereits jetzt schon nicht mehr aufgegeben werden.

Den Kleinwagen Up von VW trifft es ebenso wie den Transporter T6.1 und die Porsche-Verbrenner Macan, Cayman und Boxster: Wegen strengerer EU-Regeln für die Cyber-Sicherheit im Auto, die ab Juli gelten, verschwinden sie vom Markt, zum Teil ohne direkten Nachfolger. Bestellen lassen sich die meisten schon jetzt nicht mehr.

„Für den deutschen Markt sind bereits alle Up produziert und an den Handel ausgeliefert", erklärt eine VW-Sprecherin. In anderen EU-Ländern laufe die Auslieferung der letzten Fahrzeuge dagegen noch bis Mitte des Jahres. Dann sei auch dort Schluss. Produziert wird der beliebte Kleinwagen schon seit November nicht mehr.

Auch bei VW Nutzfahrzeuge in Hannover heißt es: „Der T6.1 ist nicht mehr bestellbar." Zwar läuft die Produktion dort noch. Doch alle Fahrzeuge, die bis Ende Juni gebaut werden können, hätten längst einen Abnehmer, sagt eine Sprecherin. „Wir sind ratzekahl ausverkauft."

Grund für den harten Schnitt: Um den neuen Regeln zur Cybersecurity, die ab 7. Juli gelten, zu entgehen, müssen die Autos bis zum Stichtag nicht nur produziert und ausgeliefert, sondern auch zugelassen sein. Dadurch habe man keinerlei Spielraum, heißt es in Hannover. Nur bei der Camper-Version T6.1 California gebe es noch letzte Bestellmöglichkeiten. Denn bei Wohnmobilen greifen die neuen Regeln erst ab 1. September.

Hoher Aufwand

Dass es vor allem ältere Modelle wie den seit 2011 gebauten Up oder den noch auf dem T5 von 2003 aufbauenden T6.1 trifft, liegt an dem hohen Aufwand, den die Hersteller betreiben müssten, um die Autos fit zu machen für die neuen Vorschriften. „Wir müssten da sonst noch einmal eine komplett neue Elektronik-Architektur integrieren", sagt VW-Markenchef Thomas Schäfer. „Das wäre schlichtweg zu teuer." Daher habe man sich entschlossen, den beliebten Kleinwagen Up ohne direkten Nachfolger einzustellen. „Leider", wie Schäfer hinzufügt. Denn gefragt sei das Einstiegsmodell nach wie vor.

In der Tat sei der Aufwand, den die Hersteller betreiben müssten, enorm, sagt Stefan Bratzel vom Center of Automotive Management (CAM) in Bergisch Gladbach. Die Kosten würden pro Fahrzeug in die Millionen gehen. Für neu entwickelte Modelle gelten die strengeren Regeln bereits seit Mitte 2022, für Alt-Modelle gab es zwei Jahre Schonfrist, die jetzt ausläuft.

Danach müssen die Hersteller nachweisen, dass es schon bei der Entwicklung der Fahrzeuge ein zertifiziertes Managementsystem zur Abwehr von Hackerangriffen gab, und das nicht nur beim Hersteller selbst, sondern auch bei Zulieferern. Das sei gerade bei sehr alten Modellen nachträglich nur

schwer zu machen, so der Autoexperte. Diesen Aufwand würden sich die Hersteller daher lieber sparen.

Volkswagen Nutzfahrzeuge (VWN) verabschiedet sich schweren Herzens vom T6.1, der bis zuletzt das meistverkaufte Modell der Marke war. „Wir hätten das Auto sicher noch zehn Jahre lang weiterverkaufen können", sagt Markenchef Carsten Intra. Doch mit den neuen EU-Regeln sei das nicht machbar. Anders als beim Up soll es hier zumindest einen Nachfolger geben, aber nicht nahtlos und nicht mehr aus Hannover: Der neue Transporter, den VWN zusammen mit Ford entwickelt hat und auch dort bauen lässt, wird erst im September enthüllt.

Porsche Boxster als Verbrenner nur noch für den Export

Bei Porsche sind die Bestellbücher für die Verbrenner-Versionen von Macan, Boxster und Cayman ebenfalls geschlossen. Produziert werden die Modelle in Leipzig und Osnabrück aber weiter – jedoch nur für den Export. In Deutschland gibt es den Macan künftig nur noch in der neuen vollelektrischen Generation, die gerade vorgestellt wurde. Den Plan, beide eine Zeit lang parallel anzubieten, musste Porsche in Deutschland aufgeben, nachdem sich der Start des Elektro-Macan wegen Softwareproblemen zwei Jahre verzögert hatte. 2025 sollen dann auch vollelektrische Nachfolger für Boxster und Cayman starten.

Auch andere Hersteller nehmen kurz vor dem Stichtag alte Modelle aus dem Programm: Audi ließ das Sportcoupé TT Ende 2023 auslaufen und schloss beim Sportwagen R8 die Bestellbücher. Mercedes-Benz stellt Ende März die Produktion des alten Zweisitzers Smart EQ Fortwo ein, der bisher parallel zum Nachfolger Smart #1 im Programm geblieben war. Renault verabschiedet sich vom Elektro-Urgestein Zoe.

Mit den neuen Regeln zur Cybersecurity habe das aber nichts zu tun, versichern alle drei. Die Modelle hätten schlicht das Ende ihres Lebenszyklus erreicht. Allerdings, so fügt ein Audi-Sprecher hinzu, werde Mitte Juni der letzte R8 ausgeliefert, damit er noch vor dem Stichtag im Juli zugelassen werden könne. Eine Zukunft hätte das Modell also ohnehin nicht gehabt.

©n-tv.de, jwu/dpa

Freitag, 1. März 2024

Schlag gegen Crimemarket

Polizei schaltet „Amazon für Cybercrime“ ab

Es war die deutschsprachige kriminelle Handelsplattform im Internet: Allein in NRW schlagen 500 Beamte zu und nehmen den 23-jährigen Betreiber fest. Auf der Plattform gab es für jeden zugänglich kriminelle Dienstleistungen sowie genaue Anleitungen zu schweren Straftaten. Jeder Nutzer muss nun mit Besuch von der Polizei rechnen.

181.000 registrierte Nutzer, 25 Millionen Euro Umsatz, sechs Festnahmen, 500 Beamte allein in NRW im Einsatz: Die Polizei hat mit mehr als 100 Durchsuchungen einen bundesweiten Schlag gegen die größte deutschsprachige kriminelle Handelsplattform im Internet geführt, wie die Ermittler in Düsseldorf berichteten. Der mutmaßliche Betreiber von „Crimemarket“, ein 23-Jähriger, sei im niederrheinischen Korschenbroich festgenommen worden. Gegen ihn werde wegen Geldwäsche und Computerbetrugs ermittelt. Den Server hätten die Ermittler in Island sichergestellt.

Die Plattform sei im Internet, nicht im Darknet, für jeden zugänglich gewesen. Entsprechend hätten auch viele Minderjährige sie genutzt, sagte Düsseldorfs Polizeipräsidentin Miriam Brauns. Es sei erschreckend, wie einfach man im Internet auf frei verfügbaren Seiten kriminelles Verhalten kaufen und beauftragen kann. Die Nutzer müssten ab heute damit rechnen, dass sich die Polizei bei ihnen meldet, sagte Brauns. „Der ‚Crimemarket‘ wurde heute geschlossen“, sagte NRW-Innenminister Herbert Reul. Man habe es „nicht mit dem kleinen Online-Händler von nebenan zu tun gehabt, sondern mit dem deutschsprachigen Amazon für Cybercrime“.

„Wir waren geschockt, was wir gefunden haben“

Auf der Plattform seien kriminelle Dienstleistungen, aber auch detaillierte Anleitungen zu schweren Straftaten oder Drogen erhältlich. Der Schlag – die letzte Datensicherung sei Freitag früh erfolgt – habe zu erheblicher Bewegung in der Szene geführt. Es habe der gesamte Datenbestand der Plattform gesichert werden können. „Anrufer haben sich gestern Abend mit verzerrter Stimme bei der Polizei in Düsseldorf und Köln gemeldet und als Journalisten ausgegeben, um an Informationen zu kommen“, berichtete Staatsanwalt Christoph Hebbecker.

Die Polizei sicherte zahlreiche Beweismittel, vor allem Mobiltelefone, IT-Geräte und Datenträger. In 21 Fällen stellte die Polizei in Nordrhein-Westfalen Drogen sicher, daneben wurden mehr als 600.000 Euro Bargeld und andere Vermögenswerte gepfändet. „Wir waren geschockt, was wir gefunden haben“, sagte Kriminaldirektor Michael Graf von Moltke. Anleitungen für Computerbetrug, Hacking, Drogenversand oder Schutzgeld-Erpressung auf Bestellung, sogar Kriegswaffen seien dort zu bestellen gewesen, auch ein Werkzeug zur Fälschung von Personalausweisen. In den Niederlanden hätten die Ermittler einen gespiegelten Server sichergestellt. Dies sei wichtig, damit die Plattform nicht wenige Stunden später wieder online gehen kann.

Gestartet sei die Plattform 2018 mit 14 Nutzern. Dann sei sie exponentiell gewachsen. Seit 2020 seien die Ermittler den Betreibern auf der Spur gewesen. Nordrhein-Westfalen sei ein Schwerpunkt der Aktion gewesen. In 33 Städten in Nordrhein-Westfalen seien 36 Durchsuchungen erfolgt, die übrigen 66 verteilen sich auf den Rest des Bundesgebiets. Von den sechs festgenommenen Verdächtigen seien drei in Nordrhein-Westfalen festgenommen worden.

©n-tv.de, jwu/dpa

Dienstag, 20. Februar 2024

„Unter Kontrolle der Behören“

Ermittler ziehen Hackergruppe Lockbit den Stecker

Die Gruppe Lockbit stellt ihre Erpresser-Software gleichgesinnten Kriminellen zur Verfügung. Weltweit werden Kommunen, Vereine und Unternehmen erpresst. Nun schlagen die Ermittler zurück.

Ermittlern ist ein großer Schlag gegen ein weltweit agierendes Netzwerk von Cyberkriminellen und Erpressern gelungen. Die Hackergruppe Lockbit ist in einer gemeinsamen Strafverfolgungsaktion der britischen National Crime Agency (NCA), des amerikanischen Federal Bureau of Investigation (FBI) und von Europol zerschlagen worden, wie aus einem Beitrag auf der ehemaligen Erpresser-Website der Bande hervorgeht. „Diese Seite ist jetzt unter der Kontrolle der National Crime Agency, die eng mit dem FBI und der internationalen Strafverfolgungseinheit ‚Operation Cronos' zusammenarbeitet“, hieß es dort weiter. Ein Sprecher der NCA bestätigte, dass die Bande zerschlagen worden sei.

Lockbit und seine Partner haben in den vergangenen Monaten einige der größten Unternehmen der Welt gehackt. Die Bande verdient ihr Geld mit dem Diebstahl sensibler Daten und der Drohung, diese weiterzugeben, wenn die Opfer nicht ein Lösegeld zahlen. Ihre Partner sind gleichgesinnte kriminelle Gruppen, die von der Gruppe rekrutiert werden, um Angriffe mit den digitalen Erpressungswerkzeugen von Lockbit auszuführen. Der US-Cybersicherheitsbehörde CISA zufolge hat Lockbit seit 2020 mindestens 1700 US-Organisationen angegriffen.

Das Bundesamt fur Sicherheit in der Informationstechnik hatte im Juni die Gruppierung, die hinter der Ransomware Lockbit steckt, als gefährlichste Cybercrime-Akteur der Welt bezeichnet. Im vergangenen August etwa war mit Sevilla Spaniens viertgrößte Stadt Ziel einer Attacke mit Lockbit geworden. Medien berichteten von Lösegeldforderungen zwischen 1,5 und 5 Millionen Euro.

Dienstag, 13. Februar 2024

„Schon von Pegasus gehört?“

Porno-Erpresser verschicken wieder mehr E-Mails

Betrüger verschicken offenbar wieder mehr E-Mails, in denen sie Empfängern drohen, peinliche Videos zu verbreiten, auf denen diese beim Masturbieren zu sehen sind. Angeblich haben sie die Geräte ihrer Opfer mit einer Spyware infiziert. Was soll man tun, wenn man eine solche Nachricht erhält?

Die Marketing-Agentur Into The Minds hat mithilfe des SEO-Tools Ahrefs von Juni 2022 bis Juni 2023 analysiert, was die Bevölkerung in den 27 EU-Staaten im Internet am meisten interessiert. An erster Stelle stehen mit 363 Millionen Suchanfragen Nachrichten, dicht gefolgt von „Inhalten für Erwachsene“ mit 351 Millionen Anfragen. Überraschend ist das nicht, auch Kriminelle wissen das und nutzen die weitverbreitete Porno-Leidenschaft für Erpresser-E-Mails. Das geht schon seit einigen Jahren so, doch aktuell sind die Cybergangster offenbar wieder besonders aktiv.

Grundsätzlich wird in den E-Mails immer die gleiche Geschichte aufgetischt: Hacker hätten den Computer oder andere Geräte mit Malware infiziert, womit sie unter anderem die Kontrolle über die Kamera erhalten hätten. Das hätten sie genutzt, um ihre Opfer beim Masturbieren zu filmen und zu fotografieren. Wenn die Empfänger nicht wollten, dass ihre Familie, Freunde, Bekannte oder Arbeitgeber die Aufnahmen zu sehen bekommen, müssten sie eine bestimmte Summe in Kryptowährung an die Erpresser schicken.

Keine Beweise, aber gut gemacht

Beweise, solch ein belastendes Material zu haben, bleiben die Erpresser schuldig. Das ist etwa bei der „Hast du schon von Pegasus gehört?“-Kampagne der Fall. Bisher verschickten die Cybergangster dafür E-Mails überwiegend auf Englisch, doch jetzt verbreiten sie die Nachricht offenbar auch zunehmend auf Deutsch.

Sie enthält recht wenig Fehler und ist weitgehend korrekt formuliert, aber man erkennt sie speziell an zu wörtlichen Übersetzungen, etwa an „Kontaktbuch“ statt „Adressbuch“. Offensichtlich nutzen die Erpresser den Google-Übersetzer. Denn wenn man ihn auf den englischen Text anwendet, entspricht das Resultat exakt dem verschickten deutschen Text, der n-tv.de vorliegt.

Der Betreff zeigt oft nicht sofort, worum es geht, sondern nutzt harmlose Formulierungen. So sollen Spamfilter umgangen werden. Ebenso häufig scheint die E-Mail vom angeschriebenen Opfer selbst zu stammen, solche Fälschungen werden Spoofing genannt.

Hohe Trefferwahrscheinlichkeit

Das Kalkül der Verbrecher ist, dass die Drohung mit der berüchtigten Pegasus-Spyware zufällig einen Empfänger trifft, der Pornoseiten besucht. Dazu malt der Text eindrücklich aus, was eine Veröffentlichung für das Leben der Betroffenen bedeuten würde. Angesichts dessen, dass Pornografie-Portale etwa so beliebt sind wie Nachrichten-Websites, ist die Wahrscheinlichkeit hoch, dass die Erpresser bei einer großen Anzahl verschickter E-Mails oft genug erfolgreich sind, um viel Geld zu kassieren.

Wie bei anderem Spam haben sie die E-Mail-Adressen gewöhnlich aus dem Darknet, wo man sie in großen Paketen günstig kaufen kann. Sie stammen unter anderem aus Hacks von Online-Portalen

oder aus den Adressbüchern von Nutzern, deren Rechner sich Malware eingefangen haben. Das kann beispielsweise passieren, wenn man einen Anhang von Spam-Mails öffnet oder einem Link darin folgt.

Noch beängstigender sind Erpresser-E-Mails, wenn sie im ohnehin schon bedrohlichen Text auch noch tatsächlich vom Opfer genutzte Passwörter, Anschriften, Telefonnummern oder andere persönliche Daten enthalten. Doch wie die Verbraucherzentrale schreibt, stammen diese Informationen gewöhnlich aus den gleichen Quellen wie die E-Mail-Adressen.

Wie soll man reagieren?

Wenn man eine Erpresser-E-Mail erhält, darf man auf keinen Fall Anhänge öffnen oder auf Links in der Nachricht klicken. Und natürlich geht man nicht auf die Forderungen der Verbrecher ein oder antwortet ihnen. Man kann die E-Mail einfach löschen oder die Behörden bei der Ermittlung der Drahtzieher unterstützen. Die Chancen, dass Letzteres etwas bringt, sind zwar gering, aber so könne man beispielsweise helfen, neue Varianten zu erkennen und gegebenenfalls Tatzusammenhänge wie Bitcoinadressen zu ermitteln, schreibt das Landeskriminalamt Niedersachsen.

Die Verbraucherzentrale rät dazu, den Erpressungsversuch über die Internet-Wache online anzuzeigen. So erscheine dieses Problem in der Kriminalstatistik und könne von den Ermittlungsbehörden ernsthaft verfolgt werden. Außerdem bittet die Verbraucherzentrale, die E-Mail an phishing@verbraucherzentrale.nrw weiterzuleiten. So könne sie Betrugsmaschen erkennen und im Phishing-Radar davor warnen.

Sollten in der E-Mail Passwörter genannt werden, die man noch verwendet, muss man sie ändern. Die von den Cybergangstern verwendete Adresse kann man auf einer Webseite des Hasso-Plattner-Instituts oder bei Have I Been Pwned? eingeben. So erfährt man, ob sie sich in einer bekannten Datenbank im Darknet befindet.

Vorbeugen ist besser

Auch wenn es höchst unwahrscheinlich ist, gibt es Fälle, in denen Kriminelle tatsächlich die Möglichkeit hatten, Nutzer über die Kameras ihrer Computer zu filmen. Um das zu verhindern, gilt es speziell auf Windows-PCs einen Virus-Schutz einzusetzen. Dieser sollte wie das Betriebssystem und andere Software aktuell gehalten werden. Programme und Apps installiert man nur aus vertrauenswürdigen Quellen.

Die Verbraucherzentrale rät zudem zu einem einfachen, aber sehr effektiven Mittel: Man soll die Webkamera abkleben, wenn man sie nicht braucht. Eleganter sind Schiebe-Blenden, die entweder am Gerät integriert oder als günstige Lösungen zum Aufkleben erhältlich sind.

©n-tv.de, hvo/dpa

Samstag, 20. Januar 2024

Attacke vor einer Woche entdeckt

Russische Hacker dringen bei Microsoft in Mails ein

Microsoft teilt mit, russische Hacker hätten sich Zugang zu Mails von ranghohen Mitarbeitern verschafft. Hinter dem Hack stehe eine Gruppe, die unter den Namen „Midnight Blizzard“ und „Nobelium“ bekannt ist.

Hacker mit Verbindungen zur russischen Regierung haben sich nach Angaben von Microsoft Zugang zu E-Mails von Mitarbeitern des Konzerns verschafft, darunter auch ranghohe Manager. Die Attacke habe im November begonnen und sei vor einer Woche entdeckt worden, teilt Microsoft mit. Die Hacker hätten zudem einige Dokumente aus E-Mail-Anhängen heruntergeladen.

Auch seien E-Mails von Mitarbeitern aus den Bereichen Cybersicherheit und Recht zur Beute der Angreifer geworden, hieß es weiter. Offen blieb, wie viele Accounts von Mitarbeitern insgesamt betroffen waren. Der Konzern machte auch keine Angaben dazu, wer aus der Konzernführung betroffen ist. Microsoft betonte, es sei ein „prozentual sehr kleiner“ Anteil gewesen. Der Konzern hatte zum Stichtag 30. Juni rund 221.000 Beschäftigte.

Die Hacker gelangten laut Microsoft ins E-Mail-System, nachdem sie das Passwort eines internen Test-Accounts geknackt hatten. Die Attacke sei keine Folge von Schwachstellen in Microsofts Produkten oder Diensten gewesen, hieß es. Es gebe auch keine Hinweise darauf, dass die Angreifer Zugang zu Kundenbereichen, Software-Quellcodes oder Systemen mit künstlicher Intelligenz gehabt hätten.

Hinter dem Hack steht Microsoft zufolge eine russische Gruppe, die unter den Namen „Midnight Blizzard“ und „Nobelium“ bekannt ist. Die Eindringlinge hätten „zunächst“ in den E-Mails nach Informationen über die Gruppe gesucht, hieß es unter Verweis auf erste Untersuchungsergebnisse. Damit könnten die Hacker besser verstehen, wie viel Microsoft über sie und ihre Vorgehensweise wisse. Microsoft machte keine Angaben dazu, wie sich der Fokus der Angreifer danach verändert habe.

Software von Microsoft wird in vielen Unternehmen und Behörden überall auf der Welt eingesetzt. Damit könnte der Hack – je nach Relevanz der erbeuteten Informationen – weitreichende Folgen haben. Bei einer der schwerwiegendsten Cyberattacken mutmaßlich russischer Hacker war vor einigen Jahren Wartungssoftware der Firma Solarwinds infiziert worden. Über sie verschafften sich die Angreifer dann Zugang in die Systeme Dutzender Firmen und Behörden.

Dienstag, 16. Januar 2024

Globales Risiken-Barometer

Hacker machen Managern die größte Angst

Weltweit haben Unternehmen wachsende Sorge vor Cyberkriminellen. Das Risiken-Barometer der Allianz-Versicherung zeigt für Deutschland allerdings interessante Besonderheiten: Auf Platz drei der Schrecken kommt hierzulande schon die Bürokratie.

Die Gefahr von Hackerangriffen und IT-Ausfällen macht den Unternehmen weltweit nach einer Studie des Versicherungsriesen Allianz im dritten Jahr in Folge die größten Sorgen. 36 Prozent der mehr als 3000 befragten Manager, Versicherungsmakler und Risikoexperten hätten Cyber-Risiken als eines der größten Risiken für ihr Unternehmen genannt, teilte die Allianz in ihrem gerade veröffentlichten jährlichen „Risk Barometer" mit. Ein Jahr zuvor waren es noch 34 Prozent.

Die Zahl der Attacken, bei denen die Daten von Unternehmen verschlüsselt werden, hätten im vergangenen Jahr drastisch zugenommen, sagte Jens Krickhahn, der Cyber-Chef der Allianz. Auch beim zweitgrößten Risiko, der Gefahr von Betriebsunterbrechungen etwa infolge gestörter Lieferketten, spielen Cyberattacken eine große Rolle. 31 (2023: 34) Prozent haben davor Angst, dass dies ihr Unternehmen treffen könnte.

Deutsche Firmen besorgt über neue Vorschriften

Auch in Deutschland hat die Angst vor IT-Risiken in der Umfrage mit 44 Prozent die Furcht vor Betriebsunterbrechungen etwa wegen Feuer, Maschinenausfällen oder Naturkatastrophen (37 Prozent) überholt. Weltweit machen den größten Sprung in der Risiko-Wahrnehmung Naturkatastrophen, die 26 (19) Prozent der Befragten beschäftigen und damit vom sechsten auf den dritten Rang vorrücken. Bei den deutschen Teilnehmern der Umfrage rangieren dagegen die Sorgen vor der Änderung von Gesetzen und Vorschriften (23 Prozent) auf Platz drei. Darunter fallen auch Sanktionen oder Zölle.

Eine besondere Rolle in Deutschland spielt offenbar der drohende Fachkräftemangel. Er wird von 20 Prozent als eines der wichtigsten Geschäftsrisiken genannt, ähnlich wie in Großbritannien, Osteuropa und Australien. Weltweit sind es nur zwölf Prozent. Vor allem IT- und Datenexperten seien schwer zu finden – was wiederum den Kampf gegen Cyber-Risiken erschwert.

„Extreme Wetterereignisse, Ransomware-Attacken oder regionale Konflikte strapazieren die Widerstandskraft von Lieferketten und Geschäftsmodellen auch in diesem Jahr", kommentiert Petros Papanikolaou, der neue Chef der Industrieversicherungs-Sparte Allianz Commercial, die Ergebnisse. An Bedeutung verloren hat für die Unternehmen weltweit laut der Studie die Angst vor makroökonomischen Einflussfaktoren wie Inflation oder steigenden Zinsen. Vor einem Jahr noch von einem Viertel der Befragten genannt und auf Rang drei gereiht, waren es diesmal nur noch 19 Prozent und Platz fünf.

©n-tv.de, mbo/dpa

Sonntag, 31. Dezember 2023

Erpressung mit Nacktbildern

Polizei erfasst Tausende Fälle von „Sextorsion“

Die deutschen Landeskriminalämter rechnen in diesem Jahr mit zahlreichen Fällen von Erpressung mit Nacktbildern oder Sexvideos. Bereits 2022 wurden Tausende Menschen erpresst. Die tatsächliche Zahl dürfte aber noch viel höher sein. Viele Opfer melden sich wohl aus Scham nicht bei der Polizei.

Tausende Menschen sind in Deutschland nach Erkenntnis der Polizei mit Nacktbildern oder intimen Videos erpresst worden. Das ergab eine Umfrage der Deutschen Presse-Agentur unter den Landeskriminalämtern. Demnach gab es 2022 weit mehr als 2000 erfasste Fälle im Inland. Allein die Polizei in Nordrhein-Westfalen sprach von 785 erfassten Taten, die als „Erpressung auf sexueller Grundlage“ über das Internet eingestuft worden seien. In Niedersachsen sind es laut LKA 109, in Sachsen-Anhalt 119, in Baden-Württemberg 308 und im Saarland 19 Fälle gewesen. Für 2023 deutet sich nach erster Einschätzung keine Trendwende an.

Die Betrugsmasche ist nicht neu. Kriminelle bringen die Geschädigten zum Beispiel in Video-Chats dazu, sich vor der Webcam auszuziehen und sexuelle Handlungen auszuführen oder intime Bilder von sich zu verschicken. Danach drohen sie laut Polizei, die Bilder oder Videos im Internet zu veröffentlichen und verlangen Geld. Die Erpressung auf sexueller Grundlage wird auch Sextortion genannt.

Bundesweite Zahlen liegen nicht vor. Nicht in allen Bundesländern werden solche Daten extra erhoben. In einigen Ländern wie Bremen und Sachsen gab es 2022 einen Anstieg innerhalb eines Jahres, im Saarland und in Mecklenburg-Vorpommern dagegen einen Rückgang. Für das zu Ende gehende Jahr liegen zumeist noch keine Angaben vor. Das Landeskriminalamt (LKA) in Sachsen-Anhalt sprach von 167 Fällen bis Mitte November, das LKA in Sachsen von 565. Die Polizei in Niedersachsen registrierte im ersten Halbjahr einen Anstieg im Vergleich zum Vorjahreszeitraum.

Hohe Dunkelziffer

Einige Landeskriminalämter gehen von einer hohen Dunkelziffer aus. Dazu hieß es vom LKA in Schleswig-Holstein: „Diese dürfte hoch ausfallen, da zu vermuten ist, dass viele Geschädigte schon allein aus Scham auf eine Anzeigeerstattung verzichten.“ Nach Einschätzung des saarländischen LKA stammten Täter aus Ländern außerhalb der EU. „Ein Hinweis hierfür ist beispielsweise, dass die Konversation in Englisch geführt wird und die Geldforderungen an Kreditinstitute ins Nicht-EU-Ausland überwiesen werden sollen.“ Die Bremer Polizei verwies vor diesem Hintergrund auf schwierige Ermittlungen und eine geringe Aufklärungsquote.

Allein in Sachsen ist in diesem Jahr bis Mitte November bereits ein Schaden von insgesamt mehr als 131.000 Euro entstanden. In Schleswig-Holstein sind es 2022 zusammen 5300 Euro gewesen. Die Polizei rät dazu, das Opfer solle im Fall einer Erpressung kein Geld überweisen, denn die Erpressung höre nach der Zahlung meist nicht auf. Vielmehr sollte Anzeige erstattet werden. Zudem sollte man nicht vorschnell Videochats zustimmen und seine Virenschutzprogramme aktuell halten. Es gebe auch Schadsoftware, die die Webcam aktivieren könne, ohne dass das Opfer dies bemerke.

©n-tv.de, joh/dpa

Dienstag, 5. Dezember 2023

Fake-Anruf im Ministerium

Habeck fällt auf russische Trolle rein

Mehrfach legen russische Trolle deutsche Politiker rein, darunter die frühere Kanzlerin Merkel. Bundeswirtschaftsminister Habeck telefoniert nun vermeintlich mit einem Vertreter der Afrikanischen Union. Ein so großer Erfolg, wie die Trolle es darstellen, sei der Fake-Anruf aber nicht gewesen, heißt es.

Auf Desinformation spezialisierte russische Trolle haben Bundeswirtschaftsminister Robert Habeck von den Grünen in ein Fake-Telefonat gelockt. Das Bundeswirtschaftsministerium bestätigte, dass es ein entsprechendes Gespräch gegeben habe. Der Anrufer gab sich nach Angaben des Ministeriums in dem Telefonat als Vertreter der Afrikanischen Union aus.

Sicherheitsrelevante oder vertrauliche Informationen seien nicht Teil des Gesprächs gewesen, hieß es weiter aus dem Ministerium. Das Telefonat sei aufgrund technischer Probleme mit der Leitung mehrmals unterbrochen worden, so dass ein zusammenhängendes Gespräch nicht zustande gekommen sei. Eine vier Minuten lange Aufnahme, die die beiden Trolle auf Telegram veröffentlichten, ist nach Angaben eines Ministeriumssprecher ein Zusammenschnitt. Weder das dargestellte Gesamtgespräch, noch die dort gestellten Fragen sowie die angefügten Antworten ließen sich bestätigen, so der Ministeriumssprecher.

Insbesondere deckten sich die Fragen weder im Tonfall, bezüglich des Akzents des Fragestellers noch im Inhalt mit den Erinnerungen an das Gespräch, hieß es. In dem angeblichen Mitschnitt ist unter anderem zu hören, wie Habeck auf Englisch ruhig erklärte, dass der Ukraine dabei geholfen werden solle, trotz russischer Angriffe ihr Getreide zu exportieren.

Das Ministerium erhielt kurz nach dem Anruf nach eigenen Angaben Hinweise der deutschen Nachrichtendienste. Diese hätten darauf hingewiesen, dass es eine Kontaktaufnahme unter falscher Identität und einen daraus resultierenden Fake-Anruf bei Habeck gegeben habe. Das Ministerium habe daraufhin den Sachverhalt analysiert und ihn zugeordnet. Der Vorfall sei zum Anlass genommen worden, die bestehenden Sicherheitsschleifen zu prüfen und zu schärfen.

Die Aufnahme wurde auf dem Kanal des kremltreuen Duos Wowan und Lexus veröffentlicht. Die beiden sind bekannt für sogenannte Pranks von ausländischen Politikern und anderen berühmten Persönlichkeiten. Unter ihren Opfern waren schon die frühere Bundeskanzlerin Angela Merkel und der britische Ex-Verteidigungsminister Ben Wallace.

Merkel war im Februar dieses Jahres nach Angaben von Wowan und Lexus auf ein inszeniertes Telefonat zum Ukraine-Konflikt reingefallen. Die kremlnahen Interviewer veröffentlichten Auszüge daraus. Merkels Büro in Berlin bestätigte damals, dass es ein Telefongespräch gab. „Ich kann ein Telefonat mit einem Anrufer bestätigen, der sich als der frühere (ukrainische) Präsident Petro Poroschenko ausgegeben hatte“, teilte eine Sprecherin mit.

Donnerstag, 12. Oktober 2023

Laut Google noch nicht vorbei

Internet-Riesen melden bislang größte Cyber-Attacke

Seit August sehen sich Amazon und Co. mit einer gewaltigen Cyber-Attacke konfrontiert. So habe es innerhalb von zwei Minuten mehr Anfragen gegeben, als Wikipedia-Artikel im gesamten September aufgerufen wurden, schreibt Google. Laut der Alphabet-Tochter dauert der Angriff immer noch an.

Große Internet-Konzerne haben nach eigenen Angaben den bislang größten Cyberangriff der Geschichte abgewehrt. Dabei handele es sich um einen sogenannten Distributed Denial of Service (DDoS), teilten Amazon, Cloudflare und die Alphabet-Tochter Google am Mittwoch mit.

Bei einer DDoS-Attacke werden Webseiten-Server mit Anfragen geflutet, bis sie in die Knie gehen. Die jüngste DDoS-Attacke sei siebenmal größer als der bisherige Rekord aus dem vergangenen Jahr, schrieb Google in einem Blog-Eintrag. „Während dieses Angriffs wurden binnen zwei Minuten mehr Anfragen generiert als Aufrufe von Wikipedia-Artikeln im gesamten Monat September."

Die Cybersicherheitsfirma Cloudflare sprach von einem um den Faktor drei größeren Angriff als zuvor jemals beobachtet. AWS, die Cloud-Sparte des Online-Händlers Amazon, bezeichnete den Angriff als „neue Qualität von DDoS-Ereignissen". Den Unternehmen zufolge begann die Attacke im August. Google sagte, sie sei noch nicht beendet.

Ein Urheber der Angriffe konnte wie so oft bislang nicht identifiziert werden. Er soll eine Schwachstelle im Internet-Protokoll „HTTP/2" ausgenutzt haben. Daher sollten Webseiten-Betreiber die Software ihrer Server auf den neuesten Stand bringen, um diese Sicherheitslücke zu schließen.

Bei DDoS-Attacken werden üblicherweise keine Daten gestohlen. Allerdings sind die betroffenen Internet-Seiten dann nicht mehr oder nur eingeschränkt erreichbar. In den vergangenen Tagen traf es unter anderem viele israelische Online-Auftritte. Im September wurde die deutsche Finanzaufsicht BAFIN ein Opfer.

©n-tv.de, maul/AFP

Samstag, 7. Oktober 2023

Hacker erbeuten Millionen Daten

Gästelisten von Motel One landen im Darknet

Wer seit 2016 in der Hotel-Kette Motel One abgestiegen ist, muss mit der Preisgabe persönlicher Angaben im Darknet rechnen. Eine Hackergruppe wollte damit Lösegeld erbeuten. Warum der Konzern die Kundendaten massenhaft speicherte, ist allerdings bislang nicht beantwortet.

Nach einem Hackerangriff auf die Hotelkette Motel One sind einem Medienbericht zufolge Namen und Reisedaten von Millionen von Kunden im Internet gelandet. Nach Recherchen der „Süddeutschen Zeitung" (SZ) enthält der knapp sechs Terabyte große Datensatz annähernd vollständige Übernachtungslisten der vergangenen Jahre seit 2016. Auch private Rechnungsadressen, Geburtsdaten von Kunden, interne Geschäftszahlen und einige Handynummern von Mitarbeitern sind demnach online zu finden.

Die Hotelgruppe mit Sitz in München hatte am 30. September im Onlinenetzwerk X, ehemals Twitter, bestätigt, Ziel eines Hackerangriffs gewesen zu sein. Dem Bericht der SZ zufolge hatte sich die Hackergruppe ALPHV zu der Attacke bekannt, mit der mutmaßlich Geld erpresst werden sollte. Motel One erklärte auf Anfrage der Zeitung, dass der Vorfall von IT-Sicherheitsexperten untersucht werde. Zudem sei eine Strafanzeige gestellt worden. Die Übernachtungsdaten stammten dem SZ-Bericht zufolge von sogenannten Notfall-Listen, die Hotels der Kette täglich anlegen. Auf die Frage, warum diese Angaben offensichtlich über Jahre gespeichert wurden, gab Motel One auf SZ-Anfrage keine Antwort.

Löschkonzept wird jetzt überprüft

„Daten sind dann zu löschen, wenn diese nicht mehr erforderlich sind und es keine gesetzlichen Aufbewahrungsfristen mehr gibt", sagt eine Sprecherin des Bayerischen Landesamts für Datenschutzaufsicht. Die Behörde wurde vor einem Monat von Motel One über das Leck informiert. „Unsere Ermittlungen sind gegenwärtig noch nicht abgeschlossen", teilte die Sprecherin mit. Zu den Standardprüfungen bei Datenschutzvorfällen gehöre auch die Überprüfung des Löschkonzepts des betroffenen Unternehmens, sagte sie.

Der Gründer und Miteigentümer der Kette, Dieter Müller, dessen Daten ebenfalls in dem Leak veröffentlicht wurden, forderte angesichts des massiven Datenlecks die Politik auf, die Cyberabwehr erheblich aufzurüsten. „Leider hat der Staat noch keinen Weg gefunden, seiner staatlichen Hoheitsaufgabe gerecht zu werden und seine Bürger und Unternehmen vor kriminellen digitalen Angriffen zu schützen", zitierte die SZ den Geschäftsmann.

©n-tv.de, rwe/dpa

Montag, 4. September 2023

Hackerangriff auf BAFIN

Webseite der Finanzaufsicht „nur eingeschränkt erreichbar“

Nach einem Hackerangriff am 1. September 2023 hat die Finanzaufsicht BAFIN Probleme mit der Erreichbarkeit ihrer Webseite. Die Finanzaufsicht teilt mit, dass sie seither intensiv daran arbeite, den Schaden zu beheben.

Die Finanzaufsicht BAFIN hat mit den Folgen eines Hackerangriffs auf ihre öffentliche Webseite zu kämpfen. „Aufgrund eines Distributed Denial of Service (DDoS) -Angriffs ist die Webseite der Bundesanstalt für Finanzdienstleistungsaufsicht (BAFIN) seit Freitag, dem 1. September 2023, nur eingeschränkt erreichbar“, teilte die Behörde auf Anfrage mit.

Denial of Service – oder kurz DoS – bedeutet so viel wie „etwas unzugänglich machen“ oder „außer Betrieb setzen“, wie das Bundesamt für Sicherheit in der Informationstechnik erläutert. Bei DoS-Attacken werde ein Server „gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht“. Bei einer DDoS-Attacke kommt anstelle von einzelnen Systemen eine Vielzahl von unterschiedlichen Systemen in einem großflächig koordinierten Angriff zum Einsatz. In der Regel sind solche Attacken keine Angriffe, bei denen es den Hackern gelingt, sich Zugang zu internen IT-Systemen zu verschaffen.

Die BAFIN habe „Sicherheitsvorkehrungen getroffen und unmittelbar nach Einsetzen des Angriffs Abwehrmaßnahmen in Gang gesetzt, die auch greifen“, teilte die Finanzaufsicht mit. Diese Maßnahmen führten jedoch dazu, dass die Website auch am Montag zeitweise nicht erreichbar sei. Die BAFIN arbeite intensiv daran, auch während des noch laufenden Angriffs, eine vollständige Erreichbarkeit ihrer Webseite wiederherzustellen. „Alle anderen Systeme der Bafin funktionieren uneingeschränkt“, betonte die Finanzaufsicht.

©n-tv.de, spl/dpa

Mittwoch, 16. August 2023

BKA veröffentlicht Lagebild

Cyber-Angriffe aus dem Ausland nehmen deutlich zu

203 Milliarden Euro Schaden verursacht Cyberkriminalität im vergangenen Jahr in Deutschland – doppelt so viel wie noch 2019. Dabei nehmen die digitalen Attacken, bei denen die Täter aus dem Inland agieren, zwar ab. Dafür wird die deutsche IT immer öfter aus dem Ausland angegriffen.

Die Gefahr schadensreicher Angriffe auf die IT-Strukturen deutscher Unternehmen und Privatpersonen ist nach Einschätzung des Bundeskriminalamtes weiterhin sehr hoch. Der in der Kriminalstatistik des Vorjahres ausgewiesene Rückgang inländischer Cybercrime-Fälle um 6,5 Prozent bedeute keine Entspannung, sagte BKA-Vizepräsidentin Martina Link bei der Vorstellung des Lagebilds Cyber-Kriminalität 2022. Der Digitalverband Bitkom verwies auf die von Computer-Angriffen hervorgerufenen Schäden, die laut einer Studie des Verbandes im vergangenen Jahr 203 Milliarden Euro betragen hätten, rund doppelt so viel wie 2019.

Link wies auf die Internationalität dieser Kriminalitätsform hin. Letztlich könnten deutsche Unternehmen von jedem Punkt der Erde angegriffen werden. Ergänzende Daten zeigten, dass die Angriffe aus dem Ausland, die nachweislich einen Schaden in Deutschland hervorgerufen haben, um acht Prozent zugelegt hätten. Sie sind in den 136.865 registrierten Fällen nicht erfasst, da diese Statistik nur Fälle erfasst, bei denen der Aufenthaltsort des oder der Täter bekannt ist und im Inland liegt.

Dabei gewinnt Cybercrime bei Auslandstaten enorm an Bedeutung. Während die digitalen Angriffe, bei denen sich der Täter in Deutschland befindet, 2,4 Prozent aller Straftaten ausmachen, ist es bei den Auslandstaten rund zehnmal so hoch. Fast ein Viertel aller registrierten Auslandstaten betreffen den Bereich Cybercrime, wie aus dem Lagebericht hervorgeht.

Mehrheit der Unternehmen für mehr Befugnisse der Polizei bei Cybercrime

Allerdings geht die Polizei davon aus, nur von etwa jeder zehnten Tat der Kriminellen zu erfahren. „Unsere Statistiken können nur die Spitze des Eisbergs erfassen“, sagte Link. Verstärkt wurden auch Kommunen und Forschungseinrichtungen ausgespäht und angegriffen. Insbesondere Ransomware-Angriffe könnten die Existenz von Unternehmen bedrohen, warnten BKA und Verband. Dabei werden mit Schadprogrammen ganze Datenbanken und IT-Systeme lahmgelegt.

Das BKA verwies auf eine globale Studie des Cybersecurity-Unternehmens Coveware, derzufolge 41 Prozent der nach einem derartigen Angriff erpressten Unternehmen ein Lösegeld gezahlt hätten. Der von der Erpressern zur Lösung angebotene Schlussel funktioniere häufig nicht, warnte Bitkom-Präsident Ralf Wintergerst.

Nach einer aktuellen Bitkom-Umfrage erwarten rund zwei Drittel (63 Prozent) der befragten Unternehmen einen Cyberangriff in den kommenden zwölf Monaten, aber nicht einmal die Hälfte von ihnen (43 Prozent) sieht sich gut genug dafür gerüstet. Zugleich befürchten 48 Prozent, dass bei einem erfolgreichen Cyberangriff ihre Existenz bedroht sein könnte. 91 Prozent fordern eine bessere Ausstattung, 90 Prozent mehr Befugnisse für die Polizei.

Grenzen der Strafverfolgung

BKA und Bitkom warben für zusätzliche Investitionen in die IT-Sicherheit und für eine vertrauensvolle Kooperation zwischen Unternehmen und Sicherheitsbehörden. Die Polizei wolle mit ihren Ermittlungen die Unternehmen nicht lahmlegen, sagte Link. Es gehe aber darum, nicht nur den Einzelfall zu beenden, sondern auch die verantwortlichen Täterstrukturen ausfindig zu machen.

Die BKA-Vize machte auf die Grenzen der Strafverfolgung einzelner Täter aufmerksam, die aus sicheren Häfen agieren könnten. Zunehmende Bedeutung komme daher der Zerstörung krimineller Infrastruktur zu, wie sie bei der Zerschlagung der Schadsoftware Emotet oder der illegalen Verkaufsplattform Hydra Market gelungen sei. Im März diesen Jahres sei es gelungen, den Bitcoin-Mixer Chipmixer zu zerschlagen und Bitcoins aus kriminellen Geschäften in Höhe von rund 90 Millionen Euro zu sichern.

Mittwoch, 16. August 2023

Der Tag

Cybercrime-Rate erschreckend hoch

Die Gefahr schadensreicher Angriffe auf die IT-Strukturen deutscher Unternehmen und Privatpersonen ist nach Einschätzung des Bundeskriminalamtes weiterhin sehr hoch. Der in der Kriminalstatistik des Vorjahres ausgewiesene Rückgang inländischer Cybercrime-Fälle um 6,5 Prozent bedeute keine Entspannung, sagt BKA-Vizepräsidentin Martina Link bei der Vorstellung des Lagebilds Cyber-Kriminalität 2022.

Der Digitalverband Bitkom verwies auf die von Computer-Angriffen hervorgerufenen Schäden, die laut einer Studie des Verbandes im vergangenen Jahr 203 Milliarden Euro betragen hätten, rund doppelt so viel wie 2019. Link wies auf die Internationalität dieser Kriminalitätsform hin. Letztlich könnten deutsche Unternehmen von jedem Punkt der Erde angegriffen werden. Ergänzende Daten zeigten, dass die Angriffe aus dem Ausland, die nachweislich einen Schaden in Deutschland hervorgerufen haben, um acht Prozent zugelegt hätten.

Ohnehin geht die Polizei davon aus, nur von etwa jeder zehnten Tat der Kriminellen zu erfahren. „Unsere Statistiken können nur die Spitze des Eisbergs erfassen“, so Link.

©n-tv.de, jws/dpa

Montag, 19. Juni 2023

Rheinische Post Mediengruppe

Hackerattacke auf Medienhaus – Zeitungen mit Notausgaben

Am Freitag wird die IT der Rheinischen Post Mediengruppe von Cyberkriminellen angegriffen. Zu Beginn der neuen Woche sind die Folgen noch immer spürbar. Viele Zeitungen erscheinen in reduziertem Umfang. Daten sollen die Angreifer nach Unternehmensangaben nicht erbeutet haben.

Bei der Rheinischen Post Mediengruppe sind zum Wochenstart nach einem Cyberangriff auf den hauseigenen IT-Dienstleister Notausgaben der betroffenen Zeitungen erschienen. Leider könne man die gedruckte und die digitale Ausgabe nicht in der gewohnten Struktur anbieten, steht auf dem Titel der „Rheinischen Post". Nach aktuellem Stand seien keine Daten entwendet worden, hieß es weiter. Das gilt demnach auch für die Daten der Kunden.

Einzelne technische Systeme hätten wegen des kriminellen Angriffs abgeschaltet, die Verbindung zum Internet gekappt werden müssen, hieß es bei der „Rheinischen Post". Die zu der Mediengruppe gehörende „Aachener Zeitung" richtete sich auf der ersten Seite an die Leserinnen und Leser und schrieb von einer Notausgabe, „die nicht vollumfänglich dem entspricht, was Sie von uns gewohnt sind".

Der Bonner „General-Anzeiger" reagierte mit einer Ausgabe, die „nicht im gewohnten Umfang und in der üblichen Aktualität" erscheine. Auch die Nachrichtenportale der betroffenen Zeitungen sind nur eingeschränkt erreichbar.

Die Störung dauert laut dem Verlag seit Freitagabend an. „Wir haben rechtzeitig reagiert. An der Lösung der Probleme arbeiten wir rund um die Uhr, und wir kommen voran", hieß es bei der „Rheinischen Post".

Montag, 12. Juni 2023

Der Tag

Studie: Jede zehnte Firma von Hackern attackiert

Elf Prozent der Firmen in Deutschland sind einer Studie zufolge im vergangenen Jahr Opfer von Hackerangriffen geworden. Das geht aus der TÜV-Cybersecurity-Studie hervor. Phishing und Erpressungssoftware seien dabei die häufigsten Angriffsmethoden. Demnach gaben 57 Prozent der befragten Sicherheitsbeauftragten von Firmen an, dass sie ihre Unternehmen von organisierter Cyberkriminalität bedroht sehen. Die Zahl der Hackerattacken habe sich seit dem russischen Angriff auf die Ukraine deutlich erhöht, sagt TÜV-Verbandspräsident Johannes Bußmann. Der Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), Gerhard Schabhuser, spricht von einer „dramatischen Professionalisierung" der Angreifer. Beide betonen, dass dabei auch Künstliche Intelligenz eine immer größere Rolle spiele.

©n-tv.de, chl/dpa

Montag, 22. Mai 2023

Nach Tagen wieder erreichbar

Cyberangriff trifft ATU empfindlich

Ein Angriff auf Server von ATU legt verschiedene Systeme der Werkstattkette lahm. Per Telefon und Schritt für Schritt auch online können Kunden das Unternehmen nun wieder erreichen. Gelöst ist das Problem aber noch nicht.

Nach einem Cyberangriff bei der Werkstattkette ATU sind die Filialen inzwischen telefonisch wieder erreichbar. Das komplette Online-Angebot des Unternehmens werde schrittweise wieder hochgefahren, sagte ein Sprecher von ATU Deutschland.

„Wir arbeiten weiterhin mit internen und externen Experten intensiv an der Behebung der IT-Störung", teilte der Sprecher mit. „Gleichzeitig haben wir mehrere Übergangslösungen installiert, um die wichtigsten Prozesse vor Ort durchführen zu können." Wann die IT-Systemstörungen vollständig behoben seien, könne man derzeit nicht absehen. Neue Erkenntnisse zu den Tätern gebe es nicht, sagte eine Polizeisprecherin.

Nach dem Angriff auf verschiedene Server des Unternehmens mit Sitz in Weiden in der Oberpfalz am vergangenen Donnerstag funktionierten verschiedene Systeme gar nicht mehr oder nur einschränkt. Der Filialbetrieb blieb nach Angaben von ATU zwar gesichert, die Kunden mussten aber mit „verschiedenen Einschränkungen rechnen". Der Internetauftritt von ATU Deutschland war am Freitag zunächst nicht erreichbar. Auch die telefonische Erreichbarkeit war betroffen.

550 Filialen und 10.000 Mitarbeiter

Die Autowerkstattkette ATU, die auch Autozubehör, Ersatzteile und Reifen verkauft, gehört zur französischen Mobivia-Gruppe und betreibt nach eigenen Angaben rund 550 Filialen in Deutschland und Österreich. Das Unternehmen beschäftigt demnach etwa 10.000 Mitarbeiter und erwirtschaftet etwa eine Milliarde Euro Umsatz pro Jahr.

Hackerangriffe treffen immer wieder Unternehmen wie Kunden. Im Februar waren beispielsweise die Websites mehrerer deutscher Flughäfen zeitweise nicht erreichbar. Vermutet wurde eine sogenannte DDos-Attacke, bei der Server gezielt mit so vielen Anfragen bombardiert werden, dass das System die Aufgaben nicht mehr bewältigen kann. Es handelt sich um eine vergleichsweise primitive Form eines Cyber-Angriffs, Daten werden in der Regel nicht abgegriffen. Seit Beginn des russischen Angriffs auf die Ukraine häuften sich solche Fälle in Europa.

Freitag, 21. April 2023

Cisco-Manager Uwe Peter

„Wir bekommen 5 Millionen Phishing-Mails am Tag“

Die Fälle von Cyberattacken steigen rasant. Der Netzwerkbetreiber Cisco hat selbst bittere Erfahrungen gemacht. Deutschland-Chef Peter warnt vor zunehmenden Attacken auf deutsche Unternehmen und fordert eine „Allianz der Guten“ gegen die Gefahr aus dem Netz.

Es vergeht kaum ein Monat ohne Cyberattacke auf ein deutsches Unternehmen – und viele davon sind erfolgreich. Vor allem Ransomware-Angriffe, bei denen die Hacker Daten verschlüsseln und nur gegen Geld wieder freigeben, nehmen Jahr für Jahr zu.

Sich dagegen zu wehren, erfordert Investitionen und Einsatz, den nicht alle zu leisten bereit sind. „Knapp die Hälfte der Unternehmen ist schlecht aufgestellt“, sagt Uwe Peter, Deutschland-Chef des US-IT-Konzerns Cisco, im Podcast „Die Stunde Null“. „Das ist besorgniserregend.“

Als Netzwerkausrüster bekommt Cisco es oft an vorderster Front mit den Cyberkriminellen zu tun. „Wir bekommen 5 Millionen Phishing-Mails am Tag“, sagt der Manager – auch wenn die in aller Regel schon von der Konzern-IT abgefangen werden. Doch selbst bei Cisco haben es Angreifer im Jahr 2022 schon über die erste Schwelle geschafft. Mit einer Phishing-Attacke konnten private Daten eines Angestellten erbeutet und ins Darknet gestellt werden.

Peter fordert im Kampf gegen Cyber-Angriffe eine „Allianz der Guten“. In Ländern wie Russland und China kooperierten Cyber-Kriminelle mit dem Staat und den Geheimdiensten, weshalb sich westliche Länder nur im Kollektiv dagegen zur Wehr setzen könnten. „Deutschland alleine ist nicht verteidigungsfähig“, sagt der Cisco-Manager. „Die Hacker-Gruppen kooperieren international und sind hoch spezialisiert.“

Dienstag, 1. März 2022

Wegen Ukraine-Unterstützung

Welche russische Cyber-Rache droht Deutschland?

Aus Rache für empfindliche Sanktionen und Waffenlieferungen an die Ukraine fürchten Sicherheitsbehörden russische Hackerangriffe auf Deutschland. Gegen wen oder was könnten sich solche Attacken wenden? Wie wahrscheinlich sind sie und wie gefährlich könnte so eine Eskalation werden?

Russlands Präsident Putin hat dem Westen unverhohlen mit extremen Konsequenzen gedroht, sollte man es wagen, sich ihm in der Ukraine in den Weg zu stellen. Die Folgen würden so sein, wie man sie in der Geschichte noch nie gesehen hat, sagte er. Was genau er damit meint, weiß man wie so oft bei ihm nicht genau. Die weitreichenden Sanktionen und beschlossenen Waffenlieferungen an die Ukraine könnte er aber durchaus entsprechend auslegen. Einen Atomkrieg wird er deshalb zwar kaum auslösen, aber Sicherheitsexperten sehen eine relativ große Gefahr, dass sich Putin mit Cyberattacken rächen könnte.

Sicherheitsbehörden bereiten sich vor

Dass der russische Präsident nicht vor Hackerangriffen auf Behörden, Infrastruktur und Unternehmen anderer Länder zurückschreckt, hat er immer wieder bewiesen. Auch Deutschland ließ er in der Vergangenheit schon mehrmals attackieren. Für westliche Ermittler gilt es unter anderem als erwiesen, dass Moskau auch 2015 Drahtzieher der Cyberattacken auf den Bundestag war, um sich für Sanktionen nach der russischen Annexion der Krim zu rächen. Zuletzt gingen der Invasion der Ukraine offenbar von Putin angeordnete Hackerangriffe voran.

Experten schätzen die Gefahr russischer Cyberattacken auf deutsche Ziele groß ein. Bundesinnenministerin Nancy Faeser sagte vergangene Woche, „die Sicherheitsbehörden hätten Schutzmaßnahmen zur Abwehr etwaiger Cyberattacken hochgefahren".

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seinen Eigenschutz und seine Krisenreaktion gestärkt sowie das Nationale IT-Krisenreaktionszentrum aktiviert. Außerdem habe man seine Zielgruppen, darunter die Bundesverwaltung, Betreiber Kritischer Infrastrukturen und weitere Organisationen und Unternehmen sensibilisiert und zu einer erhöhten Wachsamkeit und Reaktionsbereitschaft aufgerufen, teilte die Behörde mit. Man sehe zwar aktuell keine akute Gefährdung, erkenne aber eine erhöhte Bedrohungslage.

Die Zusammenarbeit des BSI mit Verfassungsschutz, Bundeskriminalamt und anderen Behörden und Einrichtungen wird vom Nationalen Cyber-Abwehrzentrum (Cyber-AZ) koordiniert.

Es gibt viele mögliche Ziele

Grundsätzlich unterscheidet man dabei zwischen zwei Schutzbereichen. Bei den kritischen Infrastrukturen (KRITIS) handelt es sich um Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen. Deren Ausfall oder Beeinträchtigung hätte nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen.

Zur kritischen Infrastruktur gehören Wasser- und Energieversorgung, Ernährung, Finanz- und Versicherungswesen, der Gesundheitssektor, Informationstechnik und Telekommunikation, Transport und Verkehr, Staat und Verwaltung, Medien und Kultur und seit dem vergangenen Jahr auch die Siedlungsabfallentsorgung.

Der zweite Bereich sind Unternehmen im besonderen öffentlichen Interesse (UBI). Zu ihnen gehören Rüstungsbetriebe oder Firmen, die Produkte oder Komponenten herstellen, die bei der IT-Sicherheit staatlicher Verschlusssachen zum Einsatz kommen.

UBI sind laut BSI-Gesetz außerdem Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen des Landes gehören und daher von erheblicher volkswirtschaftlicher Bedeutung sind. Unter Umständen zählen auch deren Zulieferer dazu. Schließlich legt man noch besonderes Augenmerk auf Betriebe, wo bestimmte Mengen an gefährlichen Stoffen vorhanden sind.

Umstrittene Rolle der Bundeswehr

Auch die Bundeswehr ist mit dem Kommando Cyber- und Informationsraum (CIR) im Cyber-AZ vertreten. Ihre Rolle ist allerdings umstritten. Unter anderem gilt auch in diesem Bereich, dass die Bundeswehr nur im Krisen- und Verteidigungsfall eingesetzt werden darf, der vom Bundesparlament festgestellt werden muss.

Wann das genau der Fall ist, ist nicht eindeutig geklärt. In einem Arbeitspapier der Bundesakademie für Sicherheitspolitik heißt es, „erst wenn ein Cyberangriff in seiner Intensität und seinen Auswirkungen einem bewaffneten Angriff gleicht, kann man völkerrechtlich von einem Angriff sprechen."

Eine völkerrechtliche Definition eines „bewaffneten Angriffs" gibt es zwar nicht. Das Arbeitspapier geht jedoch davon aus, dass dies der Fall ist, wenn Cyber-Operationen zu Toten sowie großflächiger materieller Zerstörung führen.

Ohne Mandat nur Selbstverteidigung

Solange sie nicht selbst betroffen ist, ist die Abwehr von Hackerangriffen in Friedenszeiten grundsätzlich nicht Sache der Bundeswehr. Auch sogenannte Hackbacks zur Vergeltung eines Cyberangriffs sind vom Grundgesetz nur im Verteidigungsfall gedeckt, die neue Bundesregierung hat sie im Koalitionsvertrag ausgeschlossen. Nicht ganz klar ist auch, wie weit die Befugnisse des CIR zur militärischen Aufklärung gehen.

Die Rolle der Bundeswehr in der Cyber-Abwehr könnte künftig gestärkt werden. So schreibt der Präsident des Cyber-Sicherheitsrats Deutschland, Hans-Wilhelm Dünn: „Mit unserer Solidarität für die Ukraine wird auch Deutschland zum Ziel russischer Aggressionen, sei es durch Sanktionen oder Cyberattacken. Die Bundeswehr als Verteidigungsarmee muss in die Lage versetzt werden, das Land an seinen verwundbarsten Punkten zu schützen: in der kritischen Infrastruktur mit Energieversorgern, Krankenhäusern, Transportunternehmen, Banken, Medien und Kommunikationsnetzen."

Verpflichtung zum IT-Selbstschutz

Zunächst aber sind diese Einrichtungen und Unternehmen dazu verpflichtet, selbst ihre ITSicherheit zu gewährleisten. Das BSI steht ihnen dabei beratend zur Seite. Man habe seinen Eigenschutz und seine Krisenreaktion gestärkt und hat dazu das Nationale ITKrisenreaktionszentrum aktiviert, sagte ein BSI-Sprecher dem „RND". Außerdem seien die Bundesverwaltung, Betreiber kritischer Infrastrukturen und weitere Organisationen und Unternehmen sensibilisiert und zu einer erhöhten Wachsamkeit und Reaktionsbereitschaft aufgerufen worden.

Ob deutsche Behörden, Versorger oder andere systemkritische Einrichtungen und Unternehmen ausreichend vor Cyberattacken geschützt sind, gilt als fragwürdig. Im Oktober vergangenen Jahres

schrieb der Branchenverband Bitkom zum BSI-Lagebericht 2021, 86 Prozent der deutschen Unternehmen seien zuletzt durch Cyberangriffe geschädigt worden. Eine Recherche des BR und von „Zeit Online“ ergab vergangenen Sommer, dass in den vergangenen sechs Jahren mindestens 100 deutsche Ämter, Regierungsstellen, landeseigene Kliniken, Stadtverwaltungen und Gerichte Opfer von Hackerangriffen wurden.

Noch viel Luft nach oben

Man kann davon ausgehen, dass KRITIS und UBI besser geschützt sind, allerdings verpflichten sie BSI-Gesetz oder Energiewirtschaftsgesetz nur zu Mindestanforderungen. Zwar müssen sie Störungen melden. Aus der Antwort der Bundesregierung auf eine kleine Anfrage der FDP-Fraktion ging im vergangenen Jahr aber hervor, dass beispielsweise Netzbetreiber keine expliziten Meldungen zu Cyberangriffen machen müssen. Man weiß also nicht, ob eine Störung ein Fehler oder eine Hackerattacke war.

Manches Unternehmen scheint auch seine Verpflichtung zur IT-Sicherheit nicht so ernst zu nehmen, wie es vorgeschrieben ist. So haben sich die Berliner Verkehrsbetriebe (BVG) laut „Tagesspiegel“ nach jahrelanger Weigerung erst unter massivem politischen Druck bereit erklärt, im vollen Umfang mit dem BSI zu kooperieren.

Hackerangriffe benötigen Vorbereitung und Ressourcen

Hackerangriffe auf gut abgesicherte Ziele sind nicht von heute auf morgen möglich, sondern sind aufwändig und benötigen Vorbereitung. Zunächst benötige man kompetentes Personal, das auf dem Stand der Technik ist, sagt Matthias Schulze von der Stiftung Wissenschaft und Politik (SWP) in Berlin. Dazu kommt die Infrastruktur, zum Beispiel Botnetze und Commandand-Control-Server.

Systeme müssten gescannt, Schad-Software geschrieben oder vorher auch noch eine bisher unbekannte Schwachstelle entwickelt werden. Dann müsse die Schad-Software noch ins Ziel geführt werden, beispielsweise mit Phishing, so Schulze. Das klappe dann vielleicht nicht oder die Schad-Software funktioniere möglicherweise nicht wie geplant und müsse nachjustiert werden. Anschließend müssten die Hacker das System ausspähen „und erst ganz am Ende der Kette kann ich einen Effekt auslösen, also Daten löschen, Daten verschlüsseln oder ein physisches System stören, das vielleicht dranhängt.“

Warum sieht man noch nichts?

Trotzdem wundert sich der Sicherheitsforscher, „dass man bisher noch nichts gesehen hat.“ Dafür gäbe es mehrere mögliche Erklärungen, sagt er. Eventuell sehe man gar nicht, was vorgehe, vielleicht wurden Angriffe schon erfolgreich abgewehrt. Es könne aber auch sein, dass Putins Hacker nichts von seinen Plänen wussten, es gäbe ja Berichte, russische Einheiten im Feld seien von einer Übung ausgegangen.

Der russische Staat sei schließlich paranoid und teile Nachrichten und Informationen ungern. Auch die Nachrichtendienste, die die Cyber-Einheiten beherbergten, seien sich nicht grün und stünden im Wettbewerb zueinander. Das sei aber reine Spekulation, betont Schulze.

Es sei auch möglich, dass die Hacker schon Zugänge zu Systemen hätten, sie aber noch nicht eingesetzt wurden, weil Putin noch zögere, in westlichen Ländern kritische Infrastruktur anzugreifen. „Vielleicht haben sie auch keine Zugänge oder die Verteidigung war erfolgreich.“

Gefährliche Kaskadeneffekte

Entwarnung kann der Berliner Sicherheitsforscher aber nicht geben. Er glaube zwar, dass Putin die Geschlossenheit der NATO sehe und ein Cyberangriff auf Westeuropa im Sinne eines konventionellen

Angriffs interpretiert werden könnte. „Andererseits sind wir ja schon im nuklearen Säbelrasseln und damit in der Eskalationsdynamik bereits weiter“, so Schulze.

Gegenwärtig geht er davon aus, dass man sich auf einen längerfristigen Konflikt mit Moskau einstellen müsse. Russische Cyberangriffe würden künftig auf der Tagesordnung sein, beispielsweise um strategische Vorteile zu erlangen oder um die Europäische Union zu schwächen.

Schulze befürchtet, dass es dabei zu sogenannten Kaskadeneffekten kommen könnte – auch aus scheinbar banalen Ereignissen. So könne es passieren, dass beispielsweise ein Server, der die Uhrzeit von Systemen steuert, bei einem Angriff in Mitleidenschaft gezogen wird. Als Folge könne irgendwo am anderen Ende des Internets „irgendetwas Dummes passieren.“

Sehr riskanter Hacktivisten-Einsatz

Dem Sicherheitsforscher bereiten derzeit auch weniger „offizielle“ Cyberangriffe Sorgen. Für die Ukraine griffen eine IT-Armee aus Freiwilligen und die selbsternannten belarussischen Cyper-Partisanen wahllos russische Ziele an. An die Seite Putins habe sich unter anderem die kriminelle Ransomware-Gruppe „Conti“ gestellt. Wenn diese Hacker sich jetzt gegenseitig beharkten, „wird das auch unschön.“

Schulze rät deutschen Hacktivisten dringend davon ab, sich daran zu beteiligen. Es könne zu einer unkontrollierbaren Eskalation führen, und wenn die Spur einer Cyberattacke in die Bundesrepublik führe, werde dies höchstwahrscheinlich von russischer Seite als eine vom Westen konzertierte Aktion interpretiert. „Das sehe ich sehr, sehr kritisch.“

Montag, 1. März 2022

600 IT-Fachkräfte fehlen

Deutschland ungenügend gegen „Cyberkrieg“ gewappnet

3600 IT-Spezialisten sollen deutsche Ministerien und Behörden vor möglichen Cyberangriffen schützen. Allerdings sind derzeit 600 dieser Stellen unbesetzt. Angesichts eines drohenden „Cyberkrieges“ durch Russland sei das fatal, kritisiert die Linke-Digitalexpertin Domscheit-Berg.

Bei Bundesministerien und -behörden ist jede sechste Stelle für IT-Sicherheit im Kampf gegen Cyberangriffe unbesetzt. Nach einer Antwort der Bundesregierung auf eine Anfrage der Linksfraktion fehlen derzeit 600 Fachkräfte für die 3600 Stellen für IT-Sicherheit im Bereich der verschiedenen Bundesministerien, wie die „Augsburger Allgemeine“ berichtet. Im Bereich des Bundesinnenministeriums, zu dem das Bundesamt für Sicherheit in der Informationstechnik (BSI) gehört, sei sogar jede fünfte Stelle unbesetzt.

Die Linke-Digitalexpertin Anke Domscheit-Berg kritisierte die mangelnde Personalausstattung als Gefahr vor dem Hintergrund des russischen Angriffs auf die Ukraine. „Dieser erste völlig offen ausgetragene Cyberkrieg hat eine völlig neue Dimension erreicht“, sagte Domscheit-Berg der Zeitung. „Ich fürchte, er wird nicht begrenzt sein auf ukrainische und russische Einrichtungen.“

„Cyberkrieg“ „offensichtlich länger vorbereitet“

Die russische Seite habe den „Cyberkrieg“ „offensichtlich länger vorbereitet“, sagte die Linken-Politikerin. Dabei werde Schadsoftware eingeschleust und über längere Zeit zum Ausspionieren der IT-Systeme und ihrer Daten genutzt, aber erst für spätere Angriffe weiter aktiviert. Auch in Deutschland habe es bereits derartige Attacken gegeben.

„Die Bedrohung ist real und ich kann nicht verstehen, dass die Bundesregierung das Thema nicht höher priorisiert“, sagte die Bundestagsabgeordnete. „Die Gefahr durch Cyberangriffe steigt von Jahr zu Jahr, immer wieder veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik neue Rekordzahlen zu digitalen Angriffen.“

Täglich gebe es über 300.000 neue Schadsoftware-Varianten, warnte Domscheit-Berg. Ransomware-Angriffe, bei denen Systeme lahmgelegt werden, um Geld zu erpressen, seien „dabei die größte Bedrohung“. In Deutschland seien damit bereits „Krankenhäuser, Universitäten, Kommunen und ganze Landkreise lahmgelegt“ worden.

Dienstag, 18. Januar 2022

„Risikobarometer" der Allianz

Konzerne haben große Angst vor Cyberattacken

Angriffe auf die IT-Infrastruktur sind die größte Sorge von Managern weltweit. Cyberattacken hatten im vergangenen Jahr für Schäden in Billionenhöhe gesorgt. Tendenz: steigend. In deutschen Unternehmen ist die Angst vor einem anderen Vorfall noch größer. Sogar in Pandemiezeiten.

Manager und Sicherheitsfachleute weltweit sehen in Cyberangriffen die größte Gefahr für Unternehmen. Im „Risikobarometer" des zur Allianz gehörenden Industrieversicherers AGCS liegen kriminelle Hacker mit ihren Aktivitäten auf Rang eins.

Betriebsunterbrechungen, Naturkatastrophen und Pandemien folgen auf den Plätzen zwei bis vier. Das Unternehmen hat im vergangenen Herbst insgesamt 2650 Fachleute in 89 Ländern befragt. Dazu zählten über 1200 Führungskräfte großer Unternehmen mit mehr als 500 Millionen Dollar Jahresumsatz. An der Umfrage nahmen auch eigene Fachleute der Allianz teil. Bei den 351 Teilnehmern in Deutschland waren die ersten beiden Plätze vertauscht: Betriebsunterbrechung kam vor Cyberangriffen auf Platz eins.

Die zwei Hauptgefahren Cyberangriffe und Betriebsunterbrechung hängen jedoch in vielen Fällen zusammen, wie AGCS-Manager Jens Krickhahn erläuterte. Sehr stark zugenommen hat in den vergangenen Jahren die Zahl der „Ransomware"-Attacken. Mithilfe von bösartiger Verschlüsselungssoftware legen Hacker Computernetze lahm, um anschließend für die Entsperrung hohe Summen zu erpressen. Auch sehr gute IT-Sicherheitsvorkehrungen schützen nicht hundertprozentig gegen Hackerangriffe: „Die Unternehmen stecken sehr viel Geld in die Weiterentwicklung der IT-Sicherheit, aber dennoch stellen wir fest, dass Angreifer durchkommen und Unternehmen zum Teil auch enorm schädigen können", sagte Krickhahn.

Gewaltiger Schaden mit steigender Tendenz

Die Einschätzung der von der Allianz befragten Experten deckt sich mit anderen Analysen zum Thema Cyberkriminalität. So schätzt das in der IT-Branche häufig zitierte USUnternehmen Cybersecurity Ventures, dass die durch Cyberkriminalität verursachten weltweiten Schäden 2021 sechs Billionen Dollar erreicht haben. Bis 2025 könnte diese Summe demnach auf 10,5 Billionen Dollar steigen. Die immense Summe beinhaltet Datendiebstahl und -zerstörung, Finanzkriminalität, Produktivitätsverluste, Diebstahl geistigen Eigentums und andere Delikte ebenso wie die Kosten der Schadenbeseitigung.

Mitte des Jahrzehnts wären dies dann höhere Gewinne als im weltweiten Drogenhandel und eine höhere Summe als die Bruttoinlandsprodukte sämtlicher Staaten mit Ausnahme der USA und Chinas, heißt es in einer zum Jahreswechsel veröffentlichten Einschätzung des US-Unternehmens zu den Trends im kriminellen Cyberbusiness.

„Kein Unternehmen und keine Behörde ist in der heutigen Zeit vor Cyberangriffen sicher", sagt Sebastian Artz, Bereichsleiter Cyber- und Informationssicherheit beim ITBranchenverband Bitkom. „Deshalb ist es entscheidend, sich für den Ernstfall zu wappnen und sich mit dem Thema Cybersicherheit proaktiv auseinanderzusetzen. Vor allem das Thema Ransomware wird in 2022 weiter Hochkonjunktur haben." Denn unter den verschiedenen Formen der Cyberkriminalität ist Erpressung das am schnellsten wachsende Delikt. 2021 haben kriminelle Banden nach Schätzung von Cybersecurity Ventures auf diese Weise weltweit 20 Milliarden Dollar erlöst.

Dienstag, 18. Januar 2022

Bedrohung „für uns alle“

Europol zerschlägt Netzwerk von Cyberverbrechern

Ein Angriff auf die Verwaltung einer niedersächsischen Kleinstadt löst internationale Ermittlungen gegen ein Netz aus Cyberkriminellen aus. Diese nutzen einen Onlinedienst, um ihre Opfer zu erpressen. Nun können die Behörden einen großen Erfolg verbuchen.

Europäische Ermittler haben ein Netzwerk von Cyberkriminellen unschädlich gemacht und damit Schäden in Millionenhöhe verhindert. In zehn Ländern seien 15 Server ausgeschaltet worden, die die Anonymität von Kriminellen im Internet gesichert hätten, teilte die europäische Polizeibehörde Europol in Den Haag mit. Ausgangspunkt der zweijährigen Ermittlungen war ein Cyberangriff auf die Stadtverwaltung von Neustadt am Rübenberge von 2019 – nach Angaben der federführenden Polizeidirektion Hannover. Weltweit seien verschiedene Behörden beteiligt gewesen.

Laut Europol nutzten Kriminelle die Infrastruktur des Dienstes VPNLab.net für schwere Cyber-Verbrechen. VPN („virtual private network“ oder „virtuelles privates Netzwerk“) bietet Nutzern die Möglichkeit, anonym miteinander zu kommunizieren – ohne dass Außenstehende Einblick haben. Kriminelle nutzen den Service auch für den abgesicherten Zugang zum Internet.

Die Aktion fand bereits am Montag statt. Beteiligt waren neben der Polizeidirektion Hannover und der Staatsanwaltschaft Verden unter anderem Europol und die europäische Justizbehörde Eurojust, die Kontakt zu Ermittlern etwa aus den Niederlanden, Kanada, der Tschechischen Republik, Frankreich, Ungarn, Lettland und der Ukraine herstellte. Außerdem waren das FBI in den USA sowie Ermittler in Großbritannien beteiligt.

Angriff legt Verwaltung lahm

Zu den bekannten Opfern von Cyberkriminalität zählte 2019 die Stadtverwaltung von Neustadt am Rübenberge in der Region Hannover, wo Elterngeldanträge, Baupläne und vieles mehr verschlüsselt wurden. Die Verwaltung der rund 45.000 Einwohner zählenden Stadt konnte einzelne Dienstleistungen bis ins erste Quartal 2020 daher nicht anbieten.

Neben Kommunen sind auch Unternehmen betroffen. Das Ziel der Kriminellen: Gegen Lösegeld werden die Daten wieder freigegeben. Niedersachsens Innenminister Boris Pistorius sagte, der sogenannte „Takedown“ des Netzwerks zeige, „dass wir als Sicherheitsbehörden dazu in der Lage sind, schwerkriminellen Cyber-Netzwerken das Handwerk zu legen“. Der SPD-Politiker betonte: „Das schärfste Schwert gegen international agierende Verbrecher ist ein gemeinsames und eng abgestimmtes Vorgehen.“

Niedersachsens Justizministerin Barbara Havliza erklärte, Cyberangriffe seien eine reale Bedrohung – „für uns alle“. Die CDU-Politikerin sagte: „Ist die Schadsoftware erstmal im System, sind die Folgen oft katastrophal. Die Lösegeldforderungen gehen in die Millionen, der Verlust sensibler Daten kann einen riesigen Schaden verursachen.“

VPN-Anbieter im Visier

VPNLab.net bestand nach Angaben von Europol seit 2008. Der Dienst war „besonders populär bei

Cyber-Kriminellen“, wie Europol mitteilte. Der Grund: er bot auch ein doppeltes VPN mit Servern in mehreren Ländern an. Damit hätten die Dienste genutzt werden können, um Verbrechen zu begehen – ohne Angst, von den Behörden entdeckt zu werden. Laut Polizeidirektion Hannover werden VPN-Dienste von vielen Anbietern weltweit angeboten und auch für legale Zwecke genutzt, um sich vor Nachverfolgung zu schützen.

Der Provider war bei der Aufklärung verschiedener Fälle ins Visier der Ermittler geraten. Europol schätzt, dass schwere Cyber-Attacken verhindert werden konnten. Bei der über die Server verschickte Schadsoftware handele es sich um „Ryuk“ – eine Software, die von kriminellen Vereinigungen genutzt werde, um Behörden, Firmen und Einrichtungen zu attackieren und Lösegeld zu erpressen, teilte die Polizei mit. Bei Angriffen mit dieser Schadsoftware verursachten die Täter immer wieder Schäden in Millionenhöhe.

Programm verschlüsselt Daten

Bei „Ryuk“ handelt es sich laut Polizei um sogenannte „Ransomware“ („ransom“ bedeutet Lösegeld, „ware“ ist die Abkürzung für Software). Gelangt das Programm auf einen Computer oder ein Netzwerk, verschlüsselt es Fotos, Videos, Dokumente oder ganze Datenbanken. Auf dem Endgerät wird eine Text-Datei mit einer Lösegeldforderung hinterlassen. Systemkopien werden demnach ebenfalls verschlüsselt oder gelöscht.

Die Schadsoftware zu entfernen oder das System auf einen Zeitpunkt vor dem Angriff zurückzusetzen, führt dazu, dass auch bei einer Zahlung die Dateien nicht entschlüsselt werden können. Dringt die Software in ein Netzwerk ein, kann sie nach Polizeiangaben ausgeschaltete Rechner per WLAN-Verbindung einschalten, um sie zu infizieren. Der Angriff erfolge meist per Phishing-Mail – eine E-Mail mit einem Link oder einer Datei im Anhang.

„Ryuk“ werde auch als Service angeboten – eine kriminelle Gruppe biete es einer anderen an und werde prozentual an der erpressten Beute beteiligt. Pistorius, Mitglied im Kontrollgremium von Europol, forderte erneut den Ausbau der Kompetenzen und Mittel der Behörde: „Täter agieren längst höchst dynamisch und grenzüberschreitend. Die Antwort kann nur eine starke europäische Behörde im Netzwerk der europäischen Sicherheitsbehörden sein.“

Sonntag, 12. Dezember 2021

Von Log4j-Lücke betroffen

Mehrere Behörden anfällig für Hacker-Angriffe

Beim BSI herrscht Alarmstufe Rot, seit die Log4j-Sicherheitslücke bekannt ist. Einem Bericht zufolge ist nun auch klar, dass mehrere Stellen der Bundesverwaltung potenzielles Einfallstor für Hacker-Attacken war – nach allem, was bisher bekannt ist, jedoch ohne Folgen.

Einem Bericht zufolge waren mehrere Stellen in der Bundesverwaltung wegen der schwerwiegenden Sicherheitslücke für Cyber-Angriffe verwundbar. Das haben laut „Spiegel" Überprüfungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) ergeben. Hintergrund ist die für Hackerangriffe anfällige Programmbibliothek Log4j, die bei einer einstelligen Zahl an Bundesbehörden zum Einsatz kommt.

„Bei einer Schwachstelle mit dieser Verbreitung ist auch die Bundesverwaltung betroffen", heißt es aus dem BSI. Der Behörde seien einzelne verwundbare Systeme bekannt und man habe bereits entsprechende Schutzmaßnahmen eingeleitet. Bisher liegen keinerlei Hinweise vor, dass die Schwachstelle in der Bundesverwaltung tatsächlich ausgenutzt wurde. Zumindest in einigen Fällen konnte das BSI nachvollziehen, dass die Probleme bereits behoben wurden.

Hacker können durch die Schwachstelle theoretisch eigene Schadsoftware nachladen und so Daten stehlen. Seit Freitag warnen IT-Fachleute in aller Welt, weil es sich bei Log4j um eine äußerst weitverbreitete Programmbibliothek handelt.

Am Samstag hatte das BSI die höchste, rote Warnstufe wegen der Sicherheitslücke ausgerufen. Gleichzeitig wurde laut „Spiegel" auch das IT-Krisenreaktionszentrum der Behörde aktiviert. Dabei handelt es sich um ein aufgestocktes Lagezentrum, in dem seitdem rund um die Uhr mehrere Personen mit dem Problem befasst sind.

Im nationalen Cyberabwehrzentrum ist die Schwachstelle ebenfalls thematisiert worden. Das Innenministerium sei dem Bericht zufolge mehrfach über die aktuellen Vorgänge unterrichtet worden, auch weil das Thema auf der Bundespressekonferenz am Montag eine Rolle spielen könnte. Außerdem habe eine einstellige Anzahl an Unternehmen aus dem Bereich Kritische Infrastruktur dem BSI gemeldet, dass sie von der Schwachstelle betroffen seien.

Donnerstag, 28. Oktober 2021

Spur führt nach Russland

Drahtzieher von Cyber-Erpressung enttarnt

Das Geschäft mit Erpressungssoftware boomt weltweit. Cyberkriminelle legen die Systeme großer Konzerne lahm und fordern zur Freigabe sensibler Daten ein hohes Lösegeld. Nun machen deutsche Ermittler einen dicken Fisch der berüchtigten Revil-Gruppe aus. Festnehmen können sie ihn jedoch nicht.

Strafverfolger des Landeskriminalamts Baden-Württemberg haben laut Informationen des Bayerischen Rundfunks (BR) und der „Zeit" einen mutmaßlichen Drahtzieher hinter der Schadsoftware Revil ermittelt. Bei der Software handelt es sich den Berichten zufolge um eines der berüchtigtsten Programme für Ransomware-Angriffe. In Deutschland seien unter anderem das Staatstheater Stuttgart, mehrere mittelständische Unternehmen und auch Krankenhäuser davon betroffen.

Bei Ransomware – auch als Erpressungstrojaner bekannt – handelt es sich um eingeschleuste Software, die Computer und andere Systeme blockiert. Anschließend werden die Betreiber erpresst, damit die Systeme wieder freigeschaltet werden. In dem Begriff steckt das englische Wort für Lösegeld („ransom").

Bei dem Tatverdächtigen soll es sich um einen russischen Staatsbürger handeln, der in einer Großstadt im Süden des Landes lebt. Er soll nach Ansicht der Ermittler „zweifelsfrei" der Kerngruppe von Revil und deren mutmaßlichem Vorgänger Gandcrab angehören. Reporter des BR und der „Zeit" hätten Anhaltspunkte dafür gefunden, dass der Verdächtige Geld erhalten habe, das direkt aus Ransomware-Fällen stammen soll.

Ermittler können Verdächtigen nicht festnehmen

Weder die ermittelnden Behörden – das Bundeskriminalamt und das Landeskriminalamt Baden-Württemberg – noch die Staatsanwaltschaft Stuttgart wollten sich auf Nachfrage der Medien dazu äußern. Auch der Tatverdächtige habe nicht auf Anfragen reagiert. In den Online-Netzwerken habe sich der Mann als Händler von Kryptowährungen mit luxuriösem Lebensstil präsentiert, etwa mit teuren Sportwagen, Designerkleidung und Luxusreisen. Solange er sich in Russland aufhält, könne er allerdings nicht von deutschen Strafverfolgern festgenommen werden.

Mit Ransomware wurden allein in den USA im ersten Halbjahr 2021 590 Millionen US-Dollar (rund 510 Millionen Euro) erpresst. Das geht aus einem aktuellen Bericht der US-Behörde zur Verfolgung von Finanzkriminalität hervor. Die wachsende Bedrohung durch Cyberkriminalität wird in dem Bericht betont.

Die Erpresser lassen sich meistens mit der Kryptowährung Bitcoin bezahlen. Die Auswertungen zeigen 68 verschiedene Varianten von Ransomware. Am verbreitetsten waren in den ersten Monaten dieses Jahres Revil/Sodinokibi, Conti, Darkside, Avaddon und Phobos.

Donnerstag, 21. Oktober 2021

Bericht sieht „Alarmstufe Rot“

Profi-Hacker gehen immer aggressiver vor

Mit immer dreisteren Methoden versuchen Hacker, über das Internet Geld von ihren Opfern zu erbeuten. Der aktuelle Lagebericht zur Cybersicherheit erkennt einen dringenden Handlungsbedarf seitens der Politik. Doch an konkreten Plänen scheint es noch zu mangeln.

Die Bedrohung durch Cyberangriffe ist in Deutschland deutlich gewachsen. Das geht aus dem Lagebericht 2021 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hervor, der nun veröffentlicht wurde. Darin wird die aktuelle Situation als „angespannt bis kritisch“ eingeschätzt. Ein Jahr zuvor hatte die Bonner Behörde die Lage noch als „angespannt“ charakterisiert. In Teilbereichen herrsche schon „Alarmstufe Rot“, sagt BSIPräsident Arne Schönbohm.

Ursächlich dafür seien die deutliche Professionalisierung der Cyberkriminellen, die zunehmende digitale Vernetzung und die Verbreitung gravierender Schwachstellen in ITProdukten. „Informationssicherheit muss einen deutlich höheren Stellenwert einnehmen und zur Grundlage aller Digitalisierungsprojekte werden“, heißt es in dem Bericht. Das klingt schlüssig. Aber sind die Bundesregierung und ihre Behörden dafür richtig aufgestellt?

Auf die Frage, ob es künftig ein Bundesdigitalministerium geben sollte, will der scheidende Bundesinnenminister Horst Seehofer, dessen Haus bislang die Verantwortung für das BSI und die Digitalisierung der Verwaltung trägt, nicht direkt antworten. An die Adresse der künftigen Koalitionäre sagt er nur, man werde „die allgemeine Sicherheit von der Cybersicherheit nicht trennen können“.

Perfide Methoden

Nach Einschätzung des BSI nutzen Kriminelle inzwischen teilweise sehr aufwendige, mehrstufige Angriffsstrategien, die früher nur in der Cyberspionage zur Anwendung kamen. Eine Methode: Während ein krimineller Hacker mit seinem Opfer über ein Lösegeld für den Zugriff auf von ihm verschlüsselte Daten verhandelt, startet er gleichzeitig einen Überlastungsangriff auf ein Ausweichsystem, das der Geschädigte nutzt, um seine Geschäftstätigkeit fortzusetzen. Oder der Täter veröffentlicht auf sogenannten Leak-Seiten erbeutete Daten, um das Opfer noch mehr unter Druck zu setzen.

Einige Angreifer gehen demnach auch auf Kunden oder Partner des Opfers zu, um den Druck zu erhöhen. Als Beispiel nennt das BSI in seinem Bericht den Fall einer psychotherapeutischen Praxis, wo nicht nur die Praxisinhaber, sondern auch deren Patientinnen und Patienten erpresst worden waren. Die Behörde ermahnt in diesem Zusammenhang alle Betroffenen, Angriffe möglichst schnell zu melden, um weiteren Schaden zu vermeiden.

Millionen verschiedene Schadprogramme

Die Zahl der registrierten neuen Varianten von Schadprogrammen lag mit 144 Millionen laut BSI um 22 Prozent über dem Wert im zurückliegenden Berichtszeitraum. Im Februar 2021 wurden nach Angaben des Bundesamtes an einem Tag 553.000 Schadprogrammvarianten entdeckt – ein neuer Spitzenwert. Zwischen Januar und Mai wurde dem Bericht zufolge eine große Zahl von Attacken registriert, bei denen Erpresser vorgaben, über Videomaterial des Opfers zu verfügen, das dieses angeblich beim Besuch einer Webseite mit pornografischen Inhalten zeige. Die Drohung: Sollte das

Opfer nicht einen vierstelligen Euro-Betrag in Bitcoin zahlen, werde das kompromittierende Video an alle Kontakte des Opfers verschickt.

„Die Schäden durch Erpressung, verbunden mit dem Ausfall von Systemen oder der Störung von Betriebsabläufen, sind seit 2019 um 358 Prozent gestiegen“, sagt Susanne Dehmel, Mitglied der Geschäftsleitung des Branchenverbandes Bitkom. Damit sich Unternehmen und auch Privatpersonen besser schützen können, sollte es ihrer Ansicht nach für alle die Möglichkeit geben, sich über die aktuelle Cyber-Bedrohungslage zu informieren. „Dazu müssen wir Echtzeit-Informationen nutzen und EU-weit in einem zentralen Dashboard sammeln – ähnlich dem Corona-Dashboard des Robert-Koch-Instituts.“

Dienstag, 24. August 2021

„Cyber Security Report 2021“

Studie ergibt steigende Sorgen um Cybersicherheit

Top-Manager und Politiker in Deutschland sehen die Bedrohungslage im Cyberraum auf einem Rekordniveau. Neben klassischen Hacker-Angriffen und Datendiebstählen fürchten sich die Entscheidungsträger vor allem vor einer Meinungsmanipulation durch gefälschte oder unrichtige Nachrichten. Das geht aus dem „Cyber Security Report 2021“ hervor, der am Dienstag von dem Meinungsforschungsinstitut Allensbach und dem Wirtschaftsprüfungsunternehmen Deloitte in Berlin veröffentlicht wurde.

Danach sehen 77 Prozent der Abgeordneten und Führungskräfte den Datenbetrug als höchstes Cyberrisiko für die Menschen in Deutschland an. Vor zwei Jahren lag dieser Wert bei 70 Prozent.

Auf ein neues Rekordhoch stieg auch die Sorge vor Fake News: 75 Prozent der Befragten sehen ein Risiko, dass die öffentliche Meinung durch gefälschte oder unrichtige Nachrichten manipuliert wird. Beschleunigt durch die Corona-Pandemie verlagere sich der Wahlkampf teilweise ins Netz. Entsprechend groß sei die Sorge um die Manipulation der öffentlichen Meinung durch Fake News.

„Information, Meinungsbildung und gesellschaftliche Debatten verändern sich durch die Digitalisierung und damit auch die demokratische Kultur“, erklärte Prof. Renate Köcher, Geschäftsführerin des Instituts für Demoskopie Allensbach. „Das bietet Chancen, bringt aber auch erhebliche Risiken mit sich, gerade auch für die Meinungsbildung vor Wahlen.“

Acht Jahre nach den Enthüllungen des US-Whistleblowers Edward Snowden, der ein weitreichendes Überwachungsprogramm durch US-amerikanische und britische Geheimdienste aufgedeckt hat, geht die Sorge der Entscheidungsträger vor einer staatlichen Überwachung zurück. Aktuell fürchten sich noch 48 Prozent der Befragten vor einer Überwachung aus Ländern wie den USA oder China. 2017 lag dieser Wert noch bei 54 Prozent. Eine Überwachung durch den deutschen Staat befürchten aktuell neun Prozent, 2017 befürchteten noch 21 Prozent eine Bespitzelung im Inland.

Montag, 31. Mai 2021

Studie

Nutzer sozialer Medien anfälliger für Cyber-Angriffe

Nutzer von sozialen Netzwerken sind deutlich anfälliger für Attacken von Cyberkriminellen als Menschen, die nicht auf Plattformen wie Facebook angemeldet sind.

Wie aus einer am Montag veröffentlichten Studie der Technischen Universität Darmstadt und eines Startups für IT-Sicherheit hervorging, erstellen Kriminelle personalisierte Betrugsmails oftmals anhand frei zugänglicher Informationen ihrer Opfer. Dazu zählten etwa Angaben zum aktuellen Job, der Ausbildung, Hobbys oder Kollegen.

Die in den Phishingmails enthaltenen zutreffenden Angaben würden die Opfer dazu verleiten, gesicherte Informationen wie Passwörter zu verraten oder auf nicht vertrauenswürdige Links zu klicken. Dabei würden dann schlimmstenfalls Schadsoftwares wie Trojaner heruntergeladen.

„Nutzerinnen und Nutzer von sozialen Medien sind als Hochrisikogruppen bezüglich Phishingangriffen anzusehen“, erklärte Anjuli Franz, Mitautorin der Studie. Einerseits gäben Social-Media-Nutzer online mehr über sich preis als andere. Andererseits reagierten sie aus Gewohnheit „direkt und automatisiert“ auf Aufforderungen und Hinweise.

Im Zuge der im April bekannt gewordenen Datenleaks bei Linkedin und Facebook seien Cyberkriminellen Daten einer großen Zahl von Nutzern „auf dem Silbertablett serviert“ worden. Nutzer sozialer Medien und Unternehmen müssten sich in den kommenden Monaten auf „besonders gemeine und gezielte Phishingangriffe“ einstellen, hieß es weiter.

Donnerstag, 20. Mai 2021

„Ist mir nicht leichtgefallen“

Pipeline-Chef räumt Lösegeldzahlung ein

Der US-Pipeline-Betreiber Colonial hat die Zahlung von 4,4 Millionen Dollar in Bitcoin an Erpresser eingeräumt, obwohl Behörden dringend von Lösegeldzahlungen abraten. Die Entscheidung sei „hochkontrovers“, aber „das Richtige für das Land“ gewesen, sagt CEO Blount.

Der Betreiber der größten US-Benzin-Pipeline Colonial hat erstmals öffentlich eine millionenschwere Lösegeldzahlung an Computer-Hacker eingeräumt. Er habe die Zahlung in Höhe von 4,4 Millionen Dollar autorisiert, sagte Colonial-Chef Joseph Blount dem „Wall Street Journal“. „Ich weiß, dass es eine hochkontroverse Entscheidung war.“

Doch das Unternehmen sei sich über das Ausmaß der verursachten Systemschäden unsicher gewesen und habe nicht einschätzen können, wie lange es dauern würde, bis die Pipeline wieder ans Netz gehen könne. Die Lösegeldzahlung sei deshalb im Interesse des Landes richtig gewesen. „Es ist mir nicht leichtgefallen“, erklärte Blount weiter.

Colonial war Ziel eines Hacker-Angriffs geworden und hatte den Betrieb der Pipeline, durch die etwa 45 Prozent aller an der US-Ostküste verbrauchten Kraftstoffe laufen, deshalb zeitweise komplett eingestellt. In Teilen der USA kam es darum in der vergangenen Woche zu Benzinengpässen und mitunter auch zu Turbulenzen an Tankstellen. Inzwischen läuft die Pipeline laut Colonial aber wieder.

Behörden warnen vor Anreizen für Erpressungen

Die Lösegeldzahlung erfolgte nach Informationen des „Wall Street Journal“ am 7. Mai in der Digitalwährung Bitcoin. Die im Gegenzug von den Hackern bereitgestellten Entschlüsselungs-Tools hätten jedoch nicht ausgereicht, um das System wieder voll herzustellen. US-Behörden raten Unternehmen dringend davon ab, Lösegeld zu zahlen, um Cyber-Kriminellen keine Anreize für Erpressungen zu bieten.

So entschied sich beispielsweise Irland bisher, im aktuellen Ransomware-Befall seiner Gesundheits-IT den Forderungen nicht nachzugeben. Der Fall von Colonial Pipeline hatte dazu geführt, dass die Erpresser der sogenannten Darkside-Gruppe sich für die sozialen Folgen des Angriffs entschuldigten. Sie hätten Geld verdienen und keine gesellschaftlichen Probleme auslösen wollen, schrieben die Erpresser, nachdem es etwa zu Benzin-Hamsterkäufen an Tankstellen kam. Was die tatsächliche Motivation hinter der Entschuldigung war, ist schwer abzuschätzen.

Etwa eine Woche nach dem bekanntgewordenen Angriff gab mutmaßlich Darkside selbst bekannt, dass die Gruppe Zugriff auf ihre erbeuteten Bitcoins und ihre Blog-Infrastruktur verloren habe. Aufgrund des Drucks aus den USA werde die Gruppe ihre Operationen einstellen. Ob das tatsächlich der Fall ist oder ob die Gruppe künftig unter anderem Namen wiederkehren könnte, ist unklar.

Montag, 3. Mai 2021

White-Hat-Hackerangriffe im produzierenden Gewerbe

„Wir waren Gott in den IT-Systemen“

Lassen sich kleine und mittelständische Betriebe im produzierenden Gewerbe von einem Hacker knacken? Der IT-Sicherheitsexperte Michael Wiesner hat es für den GDV versucht – und war erschreckend erfolgreich.

Wenn die Maschine die Fertigung selbst organisiert und intelligente Roboter Menschen bei der Fertigung zur Hand gehen, ist das Industrie 4.0. Und intelligente Lieferketten, die Material just in time dahin bringen, wo es benötigt wird, sind im produzierenden Gewerbe zunehmend so selbstverständlich wie intelligente Steuerketten, die wissen, wann sie das nächste Mal gewartet werden müssen. Doch wie gut sind die Maschinendaten vor Hackerangriffen geschützt? Sind Produktionsbetriebe bei der IT-Sicherheit genauso innovativ wie bei der Fertigung?

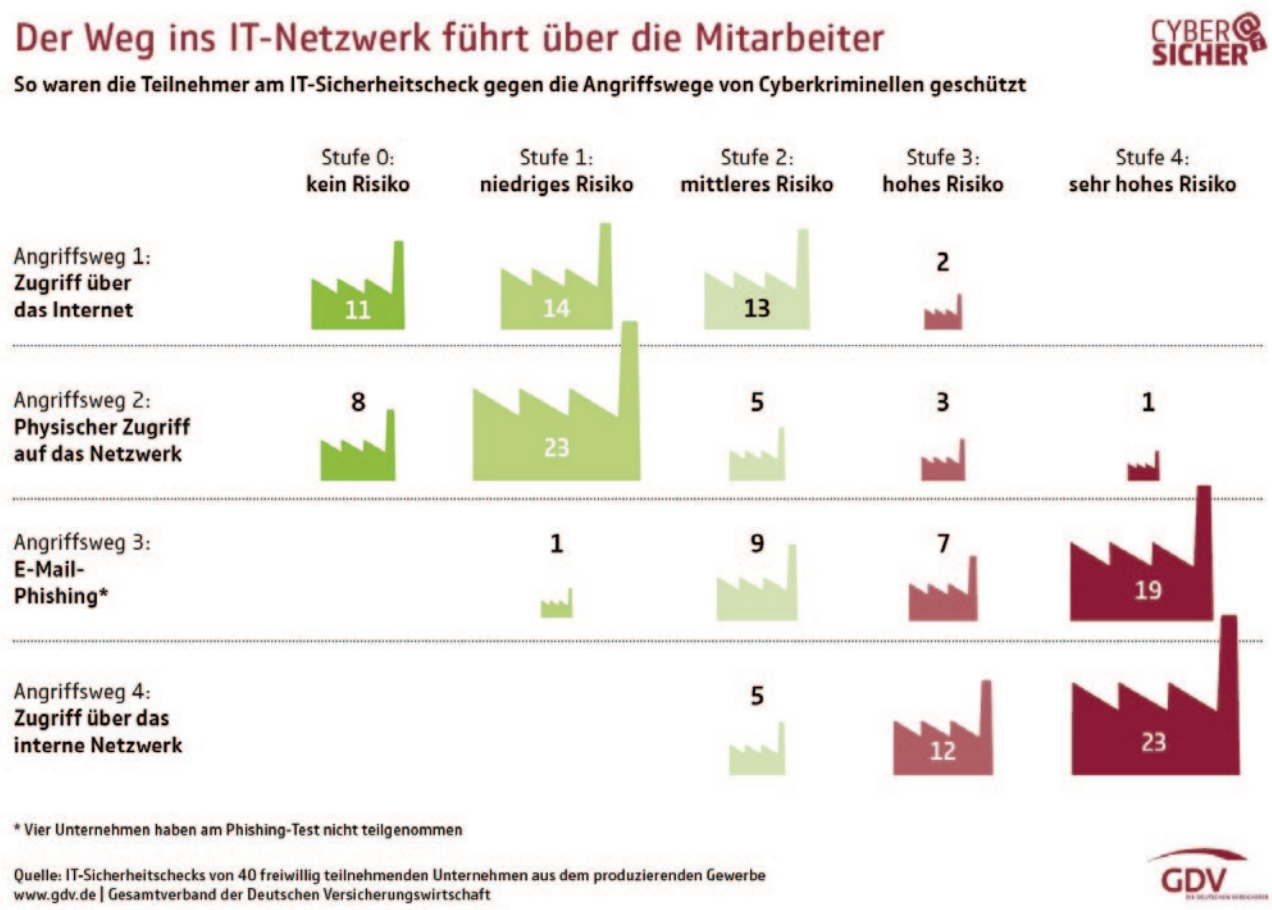
„Sagen wir es mal so: Die Eigenwahrnehmung in puncto Informationssicherheit unterscheidet sich bei sehr vielen Mittelständlern ganz eklatant von der Realität“, sagt Michael Wiesner. Als sogenannter White-Hat-Hacker wird er von Unternehmen beauftragt, um in simulierten Angriffen ihren tatsächlichen Schutz zu prüfen und auf Sicherheitslücken aufmerksam zu machen. Für den Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat er 40 kleine und mittelständische Unternehmen aus dem produzierenden Gewerbe einem mehrstufigen Stresstest unterzogen. „Das Ergebnis war insgesamt nicht schön, aber es hat mich auch nicht überrascht“, berichtet der IT-Sicherheitsexperte.

„Nicht schön” – das bedeutet im Klartext: Bei mehr als der Hälfte der Firmen konnten Wiesner und sein Team die Systeme hacken. Spielend leicht hätten sie Daten manipulieren und Maschinen übernehmen können. Ein verheerendes Fazit – vor allem, weil sich die Unternehmen freiwillig für den Test gemeldet hatten. Sie waren also vorgewarnt und hätten vorbereitet sein können. Dabei verhielten sich die IT-Sicherheitsspezialisten wie echte Cyberkriminelle, wenn sie es auf ein ganz bestimmtes Ziel abgesehen haben: Sie suchen den schnellsten Weg ins Herz der Systeme. Stufe Eins ist zunächst einmal ganz analog. Wie ist der Eingangsbereich des Unternehmens gesichert? Gibt es dort Möglichkeiten, leicht ins Netzwerk oder an Passwörter von Angestellten zu gelangen? In einer zweiten Stufe schickten die Experten Phishing-Mails an die ganze Belegschaft. Waren sie dann erst einmal in ein System eingedrungen, erfolgte der Angriff auf alle möglichen Datenbanken und Maschinensteuerungen der Unternehmen.

Unternehmen sind Eindringlingen schutzlos ausgeliefert

Die größte Schwachstelle ist noch immer der Mensch. Allein über Phishing-Mails und gefälschte Webseiten gelangte Wiesner an die Zugangsdaten von ZOO Mitarbeiterinnen und Mitarbeitern aus 19 Firmen. In sieben weiteren Unternehmen gaben Angestellte zwar keine Daten preis – dafür klickten sie aber Links an, über die echte Cyberkriminelle leicht Schadsoftware im Firmensystem hätten installieren können. Eigentlich eine alarmierende Bilanz. Aber: „Dass Phishing so erfolgreich war, hat die wenigsten Unternehmen überrascht“, berichtet Wiesner von der Reaktion der Firmen.

Geschockt zeigten sich einige Firmen immerhin über das, was dann folgte. „Wenn wir einmal in ein Netzwerk eingedrungen waren, konnten wir dort machen, was wir wollten – wir waren praktisch Gott in den IT-Systemen“, beschreibt der White-Hat-Hacker. Das heißt: Wenn ein Angreifer einmal drin ist, geben die Systeme auch dann keine Warnung aus, wenn Anomalien auftreten. „Nicht ein Unternehmen verfügte über reaktive Maßnahmen.“



Angesichts solch eklatanter Sicherheitslücken treten die wenigen positiven Ergebnisse der Untersuchung in den Hintergrund. So war die „physische Sicherheit" bei den meisten Mittelständlern weitgehend gegeben. Netzwerk-Stecker in der Lobby oder ähnliche Einfallstore waren überwiegend gut gegen Eindringlinge abgeschirmt. Ebenfalls nur ein kleiner Lichtblick: In einigen Unternehmen gab es getrennte Kreisläufe für unterschiedlich sensible Bereiche. Im Fall eines Hackerangriffs kann das von existentieller Bedeutung sein. Gelingt es Cyberkriminellen etwa sich Zugriff auf den Mailserver zu verschaffen, könnten sie andernfalls nämlich Maschinen kapern und schlimmstenfalls die Produktion komplett stoppen. Allerdings: „Die Segmentierung der Sicherheitskreisläufe verbessert sich nur langsam", sagt IT-Sicherheitsexperte Wiesner. „Inzwischen sehen wir sie immerhin in 20 bis 30 Prozent der Unternehmen."

Drei zentrale Punkte machen Unternehmen schwach

Insgesamt bemängelt Wiesner die Geschwindigkeit, mit der sich der Sinneswandel in den Unternehmen vollzieht. Für ihn sind es drei zentrale Knackpunkte, die zu den wenig erfreulichen Ergebnissen der Studie führen: unklare Zuständigkeiten, mangelhafte Risikoeinschätzung und fehlende Ressourcen. Wenn es darum geht, wer für die Datensicherheit in der Produktion zuständig ist, schieben sich die Abteilungen nach Erfahrung des Experten die Verantwortung zu häufig gegenseitig zu. Das liege nicht zuletzt an der zunehmenden Digitalisierung der Produktionsprozesse. IT und produktionsnahe Steuerung verschmelzen also immer stärker. „In der Praxis führt das oft zu einem Kompetenzvakuum", erläutert Wiesner. „Die IT fühlt sich nicht für die Maschinensicherheit verantwortlich und die operativen Mitarbeiter fühlen sich nicht als IT-Spezialisten."

Doch sind es längst nicht die Mitarbeitenden, die in mit ihrem Verhalten für die in vielen Betrieben noch immer mangelhafte IT-Sicherheit sorgen. „Dem Management fehlt nach wie vor zu häufig die Expertise, um die richtigen Schritte in der IT-Sicherheit zu gehen", urteilt Wiesner. Teils mangele es

bei den Verantwortlichen an Vorstellungskraft, wie kreativ Cyberkriminelle sind. Und diese Fehleinschätzung bestehender Risiken hat nach Erfahrung des Experten wiederum fatale Folgen für das IT-Budget personell wie finanziell. „Wenn Sicherheitslücken bestehen, hat das nicht zwingend mit einer mangelnden Kompetenz der IT-Mitarbeiter zu tun – sondern vielmehr mit fehlendem Personal und einer zu geringen finanziellen Ausstattung."

Bei den untersuchten Unternehmen kommt im Schnitt eine IT-Kraft auf 87 Mitarbeitende. Für Mittelständler mit ZOO Beschäftigten bedeutet das, sie haben Z,Z Angestellte, die sich um die gesamten IT-Systeme des Betriebes inklusive des Maschinenparks kümmern und alles am Laufen halten müssen für Prävention und die ständige Verbesserung der IT-Sicherheit bleibt dann kaum noch Zeit. Je kleiner das Unternehmen, desto größer übrigens das Problem: Ein Drittel der untersuchten Betriebe beschäftigt gar keine eigenen IT-Kräfte – alle diese Firmen haben weniger als 100 Mitarbeiter.

Zu oft steht Sicherheit nur auf dem Papier

Was können kleine und mittelständische Unternehmen tun, um der wachsenden Gefahr durch Cyberangriffe zu begegnen? Sie müssen IT-Sicherheit leben – und das bedeutet, IT-Sicherheit muss Managementaufgabe sein, meint White-Hat-Hacker Wiesner. Ein so genanntes Information Security Management System (ISMS) kann hier ein sinnvolles Instrument sein. Ein solches Konzept definiert Regeln und Methoden, um die Informationssicherheit in einem Unternehmen zu gewährleisten. Ganz zentral dabei: Es verfolgt einen Top-Down-Ansatz ausgehend von der Unternehmensführung.

Ein ISMS nützt allerdings wenig, wenn es nur auf dem Papier steht, wie auch die aktuelle Untersuchung zeigt. Nach eigenen Angaben besitzen nämlich sechs der 40 Unternehmen Grundzüge eines ISMS, eines betreibt sogar ein vollständiges. „Ausgerechnet eines dieser Unternehmen war es, in das wir am leichtesten eindringen konnten", sagt Wiesner.

Ob mit ISMS oder ohne – schon mit eigentlich selbstverständlichen technischen Maßnahmen lässt sich eine verbesserte Sicherheit gegen Hacker erzielen. „Zum Beispiel, indem Unternehmen ihre Betriebssysteme aktuell halten, regelmäßig Sicherheitsupdates einspielen und eine Zwei-Faktor-Authentifizierung für ihre Mitarbeitenden einführen", zählt Wiesner auf. Und auch wenn die finanziellen Mittel gerade in kleineren Produktionsbetrieben endlich seien, sei IT- und Maschinensicherheit gut umsetzbar: „Ein wichtiger Faktor neben mehr Geld und mehr Personal und Konzepten wie einem Informationssicherheitsmanagementsystem ist: die Kommunikation."

Hier sind alle Mitarbeitenden gefragt. Regelmäßige Phishing-Kampagnen beispielsweise könnten Belegschaften für die Gefahren, die dort lauern, sensibilisieren. „Und: Geschäftsführung und IT-Verantwortliche müssen mehr miteinander reden." Managemententscheidungen können nur so gut sein, wie die Informationen, auf denen sie beruhen. „In zu vielen Unternehmen lebt noch das Klischee von den IT-Mitarbeitenden, die im Keller sitzen und Pizza bestellen und ansonsten die Bürotür am liebsten geschlossen halten."

© spiegel.de, Patrick Beuth

Montag, 16.Oktober 2019

Hunderte Server ausgefallen

Massive IT-Störung legt Porsche-Produktion lahm

Mehr als 200 Server von Porsche waren am Dienstag ausgefallen: Nach SPIEGEL-Informationen stand dadurch nicht nur die Produktion vorübergehend still. Ausgangspunkt war ein fehlerhafter Datenspeicher.

Der Sportwagen-Hersteller Porsche musste seine Produktion im Stammwerk in Zuffenhausen sowie in Leipzig vorübergehend einstellen. Ein massiver Serverausfall war der Grund dafür.

Am frühen Dienstagabend informierte das Porsche-Management alle Mitarbeiter weltweit per E-Mail über die IT-Störung. Demnach waren alle auf SAP-Software basierenden Prozesse betroffen. Ab Mittag seien erste Probleme gemeldet worden, in den folgenden Stunden zeigte sich das ganze Ausmaß der Störung, heißt es.

In Zuffenhausen, wo mehr als 7000 Mitarbeiter täglich rund 200 Autos vom Band lassen, kam die Fertigung durch den IT-Ausfall zunächst komplett zum Stillstand. Auch in Leipzig, wo der Panamera und der Macan gefertigt werden, kam die Produktion zum Erliegen.

Nicht nur die Herstellung, auch Ersatzteillager und Kundenprozesse fielen komplett aus. 211 Server waren von den Problemen betroffen, heißt es in der Rundmail. Eine Möglichkeit, über Ersatzserver oder andere Umwege die Produktion wieder zum Laufen zu bringen, gab es demnach zunächst nicht.

Am Dienstagabend sei die Produktion aber schrittweise wieder angelaufen, teilte ein Porsche-Sprecher dem SPIEGEL am Mittwoch mit. Ein Angriff von außen oder eine Infektion mit Schadsoftware war seinen Angaben zufolge nicht der Grund für die Störung. Ein fehlerhafter Datenspeicher war der Ausgangspunkt, präzisierte Porsche später, es habe sich also um ein Hardware-Problem gehandelt. Allerdings habe eine Software, die Auswirkungen auf weitere Systeme hätte stoppen sollen, nicht funktioniert. Der Produktionsausfall werde aber „keine nachhaltigen wirtschaftlichen Auswirkungen“ auf Porsche haben, sondern wieder aufgeholt werden.

Pilz Gruppe: „Sämtliche Computersysteme vom Netz“

Bereits am Sonntag sind beim Automatisierungsspezialisten Pilz aus Ostfildern „sämtliche Computersysteme vom Netz genommen“ worden. Das Unternehmen sieht sich anders als Porsche aber als „Opfer eines gezielten Cyberangriffs“. Betroffen seien „weltweit sämtliche Server- und PC-Arbeitsplätze inklusive des Kommunikationsnetzwerkes“, teilt die Pilz Gruppe mit . Die Störungen würden „noch einige Tage andauern“. Mehr wollte eine Unternehmenssprecherin auf SPIEGEL-Anfrage nicht dazu sagen, sie verwies auf die laufenden Ermittlungen des Landeskriminalamtes.

In den vergangenen Jahren hat Schadsoftware in verschiedenen deutschen Unternehmen vergleichbare Auswirkungen gehabt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte bereits im Dezember und zuletzt noch einmal im September von mehreren Fällen gesprochen, in denen es durch die Malware Emotet „große Produktionsausfälle“ gab, „da ganze Unternehmensnetzwerke neu aufgebaut werden mussten“.

Die Ransomware WannaCry wiederum befiel 2017 innerhalb weniger Tage weltweit rund 200.000 Rechner und sorgte für Schäden von mindestens mehreren Hundert Millionen Euro, andere Schät-

zungen gingen in den Milliardenbereich. Auch damals war ein Autohersteller betroffen: Renault in Frankreich.

Die Malware NotPetya hatte kurz darauf sogar für Schäden in Höhe von geschätzt zehn Milliarden Dollar gesorgt, indem sie sich rasend schnell verbreitete und Daten auf befallenen Rechnern unwiederbringlich verschlüsselte.

Mittwoch, 16. Oktober 2019

Pilz-Chef: „Wir werden erpresst“

IT-Ausfall: Stillstand bei Porsche und Pilz

Porsche musste wegen eines Serverausfalls die Produktion in zwei Werken stoppen. Auch Pilz leidet unter einem Ausfall der IT. Der Automatisierungsspezialist wurde Opfer eines Hackerangriffs – und erklärt im Video, was genau passiert ist.

Der Automatisierungsspezialist Pilz aus Ostfildern hat derzeit Probleme bei der IT, wie Geschäftsführer Thomas Pilz auf dem Maschinenbau-Gipfel in Berlin berichtete. Das Unternehmen wurde Opfer eines Hackerangriffs. „Wir hoffen, dass wir am Montag unsere Server wieder zum Laufen bringen können, momentan geht nix“, so Thomas Pilz gegenüber „Produktion“ auf dem Gipfeltreffen des deutschen Maschinenbaus.

Holger Paul, Leiter Kommunikation des Maschinenbauverbands VDMA, kommentierte diesen Vorfall auf Twitter: „Die bittere Ironie nach einem Cyberangriff: das BSI will dem Mittelstand nicht helfen, aber der Betriebsprüfer kommt trotzdem und will Belege sehen. Thomas Pilz schildert die Realität nach dem Hackerangriff auf seine Firma auf dem Maschinenbau-Gipfel.“

Pilz selbst machte auf dem Gipfeltreffen eine klare Ansage: Der Maschinenbauer werde kein Lösegeld an Hacker-Erpresser zahlen.

Server-Ausfall bei Porsche – Produktion stand still

Auch Porsche leidet unter IT-Problemene. Laut dem „Spiegel“ fielen bei dem Autobauer mehr als 200 Server aus. Am frühen Dienstagabend informierte das Porsche-Management alle Mitarbeiter weltweit per E-Mail über die IT-Störung. Demnach waren alle auf SAP-Software basierenden Prozesse betroffen. Ab Mittag seien erste Probleme gemeldet worden, in den folgenden Stunden zeigte sich das ganze Ausmaß der Störung, heißt es in dem Bericht.

Massiv betroffen waren die Werke Zuffenhausen und Leipzig. In beiden kam die Produktion zum Erliegen. Darüber hinaus waren auch Ersatzteillager und Kundenprozesse des Autobauers von dem Serverausfall betroffen. Eine Möglichkeit, über Ersatzserver oder andere Umwege die Produktion wieder zum Laufen zu bringen, gab es demnach zunächst nicht.

Gegenüber dem „Spiegel“ erklärte ein Porsche-Sprecher, dass es sich nicht um einen externen Hackerangriff gehandelt habe. Ein intern entstandenes Problem sei der Grund für den Produktionsstopp gewesen.

Am Dienstagabend sei die Produktion jedoch schrittweise wieder angelaufen. Zum entstandenen Schaden machte der Porsche-Sprecher zunächst keine Angaben, ebenso wenig zu den technischen Details der Störung.

Wie sich Maschinenbauer über den VDMA gegen Cyberangriffe versichern können

Um genau solche Angriffe wie bei Pilz abzusichern, hat die 100prozentige VDMA-Tochter VSMA eine speziell auf die Bedürfnisse von Maschinenbauern zugeschnittene Versicherung entwickelt.

„Diese Versicherung deckt verschiedene Bereiche ab – von Kosten durch Betriebsunterbrechung, über Schäden bei Kunden bis hin zu teilweiser Erstattung von Lösegeldern“, erklärt Jürgen Seiring von VSMA. Auch eine Notfallplanung und die Einschaltung von Forensikern zur Beseitigung der Schadsoftware sind Teil der Versicherung.

Dienstag, 2. Juli 2019

Hackerangriff

So dreist kassieren Cyber-Erpresser Lösegeld von Wempe

Kriminelle griffen Juwelier bereits vor einer Woche an. Die Firma ist nicht das erste Opfer. Polizei geht von Milliardenschäden aus.

Hamburg. Der Hamburger Traditions-Juwelier Wempe ist Opfer einer Cyber-Erpressung geworden. „Eine Gruppe professioneller Täter blockierte unser Computersystem mit einer speziellen Software. Durch diese Erpressungssoftware (sogenannte Ransomware) waren unsere Server verschlüsselt. Das war eine Geiselnahme unserer Daten auf unseren eigenen Servern", sagte Sprecherin Nadja Weisweiler auf Abendblatt-Anfrage.

Wempe-Erpressung begann vor einer Woche

Der Vorfall ereignete sich bereits am Montag vor einer Woche. Auf den Servern hatten die Erpresser eine Nachricht und eine E-Mail-Adresse zur Kontaktaufnahme hinterlassen. Die Kriminellen forderten Lösegeld. Als Gegenleistung sollte der 1878 gegründete Juwelier – mit Filialen in der ganzen Welt – ein Passwort erhalten, um wieder auf die eigenen Server und damit auf die verschlüsselten Daten zugreifen zu können.

„Naturlich haben wir umgehend das Landeskriminalamt (LKA) der Hamburger Polizei informiert, das dann die Ermittlungen aufgenommen hat", sagte Sprecherin Weisweiler. Die Server seien umgehend vom Netz genommen und externe Experten fur IT-Forensik und IT-Sicherheit hinzügezogen worden.

Ein Sprecher der Hambürger Polizei bestätigte dem Abendblatt: „Wir führen derzeit ein Ermittlungsverfahren wegen Verdachts der Erpressung und der Datensabotage zum Nachteil eines Hamburger Unternehmens. Nach dem bisherigen Erkenntnisstand wurden dabei die auf einem Server abgelegten Daten des Unternehmens angegriffen, verschlüsselt und Forderungen zu deren Wiederherstellung gestellt."

Wempe musste Rechnungen per Hand schreiben

Auf den Computern sind auch Tausende Kundendaten gespeichert. Aber auf diese hatten es die Täter offensichtlich nicht abgesehen: „Nach dem derzeitigen Stand der Analyse gibt es keine Hinweise auf die Entwendung der Daten unserer Kunden und Geschäftspartner", sagte Weisweiler.

Neben dem LKA informierte Juwelier Wempe auch den Hamburgischen Beauftragten für Datenschutz über die Cyber-Attacke. Der Geschäftsbetrieb in den weltweit 34 Niederlassungen ging trotz des Vorfalls weiter. Die Kassen waren von der Cyber-Erpressung nicht betroffen. Allerdings konnten keine Rechnungen ausgedruckt werden und wurden deshalb per Hand geschrieben. Lediglich bei der Wartung von Uhren komme es zu Verzögerungen, sagte Weisweiler.

Abendblatt exklusiv: Wempe zahlte Lösegeld

Nach exklusiven Abendblatt-Informationen bezahlte Juwelier Wempe schließlich ein Lösegeld an die Kriminellen und erhielt daraufhin das Passwort. Die Höhe ist nicht bekannt. Aktuell liege das Haupt-

augenmerk auf der Wiederherstellung der Systeme. Dabei werde vorsichtig und mit Bedacht vorgegangen, so Weisweiler. Auch der Hamburger Beiersdorf Konzern wurde in der Vergangenheit bereits Opfer einer Cyber-Attacke.

Was will die Politik?
Hamburgs FDP fordert seit Langem, dass die technische Ausstattung der Polizei verbesser werden muss, damit man diese Cyberangriffe auch zurückverfolgen kann. Ende Mai hat Justizsenator Till Steffen (Grüne) eine Bundesratsinitiative mit dem Ziel einer umfassenden Reform des Computerstrafrechts eingebracht. Die bisherige Gesetzgebung im Bereich Cybercrime sei lückenhaft, ein einziges Flickwerk. Andererseits dürfe ein modernes Computerstrafrecht auch nicht so ausgestaltet werden, dass es die Freiheiten des Einzelnen bedroht.

Wie die Erpresser via Internet vorgehen und wie sich Firmen schützen können, gibt eine kleine Übersicht:

Was ist Cyberkriminalität?

Weit überwiegend handelt es sich dabei um Computerbetrug, rund 75 Prozent aller Cybercrime-Straftaten gehen darauf zurück. Dabei greift der Täter ohne Erlaubnis in die Funktion eines Computerprogramms ein, verursacht so einen Vermögensschaden und verschafft sich selbst einen Vermögensvorteil. Weiter fallen unter Cybercrime zum Beispiel unrechtmäßige Abbuchungen von Online-Konten. Auch Computersabotage, das Ausspähen von Daten oder die missbräuchliche Nutzung von Telekommunikationsdiensten sowie Datenveränderung fallen in den Deliktbereich.

Wie gefährlich ist Cybercrime?

In kaum einen anderen Deliktbereich steigen die Fallzahlen derart rasant wie bei der Cyberkriminalität. Und doch sind die Fälle, die der Polizei gemeldet werden, nur die Spitze des Eisbergs, wie das Bundeskriminalamt (BKA) konstatiert. Die polizeiliche Kriminalstatistik gebe „nicht annähernd" die tatsächliche Häufigkeit von übers Internet gesteuerten Attacken gegen Firmen oder private Nutzer wieder. „Es muss von einem sehr großen Dunkelfeld ausgegangen werden", so das BKA. Häufig zahlen die Firmen dann lieber schweigend ein Lösegeld, als sich einem vermeintlichen Imageschaden auszusetzen. Die Täter wiederum verschleiern häufig ihre Identität und operieren anonym vom Ausland aus.

Wie gehen die Täter vor?

Insbesondere mittelständische Unternehmen sind von einem massenhaften Befall ihrer Daten und Netzwerke betroffen. Am häufigsten infizieren die Täter fremde Computersysteme mit Schadsoftware, um beispielsweise an sensible Daten zu gelangen oder um von den Unternehmen ein Lösegeld zu erpressen, indem sie durch Verschlüsselung ganze Firmennetzwerke lahmlegen und so den Zugriff sperren. Zuletzt hat der Trojaner „Emotet" der Hamburger Polizei viel Sorge bereitet. Die Schadsoftware verwendet zur Tarnung täuschend echt aussehende Mails angeblicher Freunde oder Geschäftspartner. Es gibt aber auch die Variante mit verseuchten Bewerbungsmails. Wird die angefügte Datei geöffnet, verbreitet sich die Schadsoftware mitunter im gesamten Netzwerk.

Gibt es Fälle in Hamburg?

Sehr viele. Nur die wenigsten werden aber bekannt, wie der Hackerangriff auf den Konzern Beiersdorf im Juni 2017. Vermutlich gelang es den Tätern, die Buchhaltungssoftware einer Firmenfiliale in der Ukraine während eines Updates zu manipulieren. Folge: Der Trojaner verschlüsselte wichtige Dateien und machte die Computer im Netzwerk praktisch unbenutzbar. Von einem ähnlichen Schädling

wurde auch die dänische Maersk-Gruppe im Juni 2017 heimgesucht – die gesamte digitale Infrastruktur des Reederei-Riesen brach zusammen. Die Täter verlangen dann meist ein Lösegeld zur Entschlüsselung der Dateien, zahlbar in der Krypto-Währung Bitcoin.

Wie hoch ist der Schaden?

Der Schaden durch Cybercrime kann auch aufgrund des zurückhaltenden Anzeigeverhaltens der Geschädigten nur geschätzt werden. Nach einer anonymen Befragung des Digitalverbandes Bitkom sind mittelständische Unternehmen am häufigsten von Attacken betroffen, aber auch Großfirmen und Handwerksbetriebe sind nicht davor gefeit. Laut Bitkom hat in den Jahren 2017 und 2018 ein Viertel aller deutschen Industrieunternehmen einen Angriff durch Schadsoftware registriert. Der Schaden geht in Deutschland in die Milliarden Euro, weltweit, so die Polizei, wird der Schaden durch Cyberkriminelle auf mehr als 350 Milliarden Euro geschätzt.

Operieren die Täter nur am Computer?

Nicht unbedingt. Wie akut existenzgefährdend sich digitale kriminelle Machenschaften im echten, analogen Leben auswirken können, hat eine mittelständische Hamburger Firma vor gut einem Jahr erfahren müssen: Ein Angestellter der IT, zuständig für das Computer-Netzwerk, wechselte damals zu einem Konkurrenten und brachte seinem neuen Arbeitgeber ein „Willkommensgeschenk" mit: kurz vor seinem Abgang hatte sich der Mitarbeiter noch umfassenden Zugriff auf das Netzwerk seines alten Arbeitgebers verschafft. So gelang es dem neuen Arbeitgeber, die Kommunikation des Konkurrenten auszuspähen und ihn bei Ausschreibungen regelmäßig zu unterbieten. Bevor der Betrug aufflog, stand das bespitzelte Unternehmen mit dem Rücken zur Wand.

Wie kann man sich schützen?

Die Polizei rät dazu, bei der Sicherung der IT-Infrastruktur nicht zu sparen. Besser dran sind Unternehmen grundsätzlich, wenn sie auf ein „gutes und professionell gewartetes Backup-System setzen", um im Ernstfall ihre Daten aus nicht infizierten Quellen wiederherstellen zu können, sagt Andreas Dondera, Leiter der Zentralen Ansprechstelle Cybercrime (ZAC) bei der Hamburger Polizei. Auch eine Schulung der Mitarbeiter ist entscheidend, denn in den meisten Fällen gelangt Schadsoftware überhaupt nur durch einen menschlichen Fehler ins Netzwerk. Die Polizei setzt auf Prävention, stellt für Unternehmen im Internet Tipps zur Cyber-Sicherheit zur Verfügung.

Dienstag, 8. Januar 2019

Massenhafter Datenklau

„Ärger" über Politik trieb Hacker

Der 20-jährige Verdächtige im Fall des Datenklaus bei Politikern und Prominenten ist geständig. Laut Ermittlern gibt er an, allein gehandelt zu haben. Sein Motiv: „Ärger" über die aktuelle Politik.

Der nach dem massiven Online-Angriff auf Politiker und Prominente vorübergehend festgenommene 20-jährige Deutsche hat in einer Vernehmung Ärger über Äußerungen seiner Opfer als Motiv für seine Taten genannt. Das teilte Oberstaatsanwalt Georg Ungefuk, Sprecher der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt am Main, mit.

Ermittler hatten den jungen Mann, der noch bei seinen Eltern wohnt, am Wochenende in Mittelhessen festgenommen. Laut Ungefuk handelt es sich bei dem Beschuldigten um einen „sehr computeraffinen" Menschen, der aber über keine entsprechende Ausbildung verfüge und nicht vorbestraft sei. Der Mann habe viel Zeit damit verbracht, sich am PC bestimmte Kenntnisse anzueignen. Bei der Vernehmung habe er die Tat eingeräumt und umfassend mit den Ermittlern kooperiert. Zudem habe er erklärt, dass er allein gehandelt habe. Die bisherigen Ermittlungen hätten keine Hinweise auf eine Beteiligung weiterer mutmaßlicher Täter gegeben.

Beschuldigter zeigt Reue

Der Mann wurde nach der Vernehmung auf freien Fuß gesetzt. Es gibt „eine klare Reue-Reaktion", sagte Ungefuk. Der 20-Jährige sei bei der Ausspähung und Veröffentlichung der privaten Daten möglicherweise unbedacht oder leichtfertig gewesen. Bei jüngeren Tätern erlebe man oft, dass dann, wenn plötzlich die Polizei vor der Tür stehe, doch „ein großes Nachdenken einsetzt", so Ungefuk. Derzeit werden die beschlagnahmten Datenträger untersucht. Offenbar gelang es dem 20-Jährigen noch vor der Durchsuchung der Wohnung einen Speicherträger zu vernichten. Reste des gelöschten Datenmaterials konnten aber gesichert werden.

Bei seinem Datenklau hat der 20-Jährige mehrere Sicherheitslücken ausgenutzt. Für die Tat sei ein „gewisser technischer Sachverstand" nötig gewesen, sagte Ungefuk. Dem jungen Mann sei es durch eine „ausgeklügelte Vorgehensweise" gelungen, die Daten auszuspähen. Es habe nicht nur eine, sondern mehrere Ausspähaktionen gegeben, vor allem im Jahr 2018. Zudem habe er Daten aus öffentlich zugänglichen Quellen zusammengetragen. Einige Sicherheitslücken seien inzwischen geschlossen worden.

Der 20-Jährige soll über das inzwischen gesperrte Twitter-Konto @_0rbit im Dezember zahlreiche persönliche Daten von Politikern und Prominenten als eine Art Adventskalender veröffentlicht haben. Rund 1000 Politiker, Prominente und Journalisten sind nach Angaben des Bundesinnenministeriums von dem Online-Angriff betroffen. Etwa 50 Fälle seien schwerwiegender, weil größere Datenpakete wie Privatdaten, Fotos und Korrespondenz veröffentlicht wurden.

Donnerstag, 17. Januar 2019

Millionen gestohlener Passwörter im Netz aufgetaucht

Im Internet ist ein unverschlüsselter Datensatz mit gestohlen Log-in-Informationen aufgetaucht.

Im Internet stößt ein australischer IT-Experte auf einen riesigen Datensatz mit gestohlenen E-Mail-Adressen und Passwörtern. Millionen Menschen weltweit sind von dem Datendiebstahl betroffen. Über einen kostenlosen Dienst können Nutzer überprüfen, ob sie betroffen sind.

Im Internet ist ein gewaltiger Datensatz mit gestohlenen Log-in-Informationen aufgetaucht. Darin enthalten seien knapp 773 Millionen verschiedene E-Mail-Adressen und über 21 Millionen im Klartext lesbare unterschiedliche Passwörter, berichtete der australische IT-Sicherheitsexperte Troy Hunt. Insgesamt umfasse die Sammlung mit dem Namen „Collection #1" mehr als eine Milliarde Kombinationen aus beiden.

Der 87 Gigabyte große Datensatz bündele Informationen „aus vielen einzelnen Datendiebstählen und Tausenden verschiedenen Quellen", schrieb Hunt in einem Blogeintrag. Der in der Szene sehr geschätzte Security-Experte erklärte weiter, es handle sich um den größten einzelnen Datensatz dieser Art, mit dem er bislang zu tun gehabt habe. Betroffen sind Internetnutzer weltweit – darunter auch Anwender aus Deutschland.

Wer überprüfen will, ob seine E-Mail-Adresse in der Sammlung auftaucht, kann Hunts Dienst haveibeenpwned.com nutzen. In der Datenbank wird die Adresse mit Abermillionen Informationen aus Datenlecks abgeglichen. Er habe auch die jüngsten Daten dort eingepflegt, erklärte der Microsoft-Mitarbeiter Hunt. Spätestens wenn die eigene Mail dort auftauche, solle man über ein neues Passwort und wenn möglich über eine Zwei-Faktor-Authentifizierung nachdenken, sagte Linus Neumann vom Chaos Computer Club.

Experte rät zu zufälligen Passwörtern mit maximaler Länge

„Das Jahr ist gerade mal zwei Wochen alt und es ist bereits das zweite Mal, dass wir alarmierende Nachrichten haben", sagte er auch mit Blick auf den massiven Online-Angriff auf knapp 1000 Politiker und Prominente, der Anfang Januar publik geworden war. „Es gibt keine Ausreden mehr. Jeder der nichts für seine Sicherheit macht, handelt fahrlässig und geht ein Risiko ein."

Neumann rät, bei allen Diensten ein jeweils anderes und zufälliges Passwort mit maximaler Länge zu nutzen. Dieses solle dann über einen Passwort-Manager verwaltet werden. Bei der von Neumann empfohlenen Zwei-Faktor-Authentifizierung entriegeln Nutzer den Zugang zu ihrem Onlinekonto oder Social-Media-Profil zusätzlich zum Passwort durch eine weitere Abfrage auf einem anderen Weg. Das kann beispielsweise eine SMS oder eine Code-Abfrage sein.

Laut Hunt können die Datensätze besonders für das sogenannte „Credential Stuffing" missbraucht werden. Bei dieser Methode nutzen die Angreifer die Kombination aus E-Mail und Passwort, um sich auch bei anderen Diensten – beispielsweise bei Soziale Netzwerken oder Shopping-Plattformen einzuloggen. Die Hacker gleichen dabei lange Listen mit Log-in-Daten automatisch mit den Zugangssystemen ab.

In den vergangenen Jahren hatte es diverse Hacker-Attacken gegeben, bei denen zum Teil Hunderte Millionen Kombinationen aus E-Mail-Adressen und Passwörtern erbeutet worden waren. Die Passwörter waren dabei aber größtenteils kryptografisch verschlüsselt gewesen.

Donnerstag, 11. Oktober 2018

Mehr Schadprogramme im Umlauf

Cyber-Kriminelle setzen auf neue Methoden

Kriminelle im Internet werden immer raffinierter. Sie könnten sich sogar in Herzschrittmacher einklinken und diese umprogrammieren, heißt es in einem neuen Behörden-Bericht. Um an Geld zu kommen, schwenken die Hacker demnach auf eine neue Methode um.

Cyber-Kriminelle schwenken von Erpresser-Software zunehmend auf lukrativere Aktivitäten um. Angriffe mit sogenannter Ransomware scheinen in dem Maße abzunehmen, wie andere Geschäftsmodelle wie etwa das illegale Krypto-Mining zunehmen, schreibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem jährlichen Lagebericht. Das BSI ist zuständig für die Abwehr von Cyberangriffen und berät Verbände und Unternehmen.

Bei der illegalen Variante des Krypto-Minings kapern Kriminelle mit Hilfe von Schadsoftware die Rechner, um die Kapazität für das „Schürfen" digitaler Währungen wie Bitcoin zu nutzen. Die Opfer bleiben zum Teil auf hohen Strom-Rechnungen für den erheblichen Energiebedarf sitzen. Bei Ransomware-Angriffen sperren die Angreifer hingegen bestimmte Dateien oder gar ganze Rechner und verlangen von den Betroffenen Lösegeld für die Freischaltung.

Das passierte etwa im Mai 2017 bei der weltweiten WannaCry-Attacke, bei der mehr als 300.000 Computer in 150 Ländern infiziert wurden, darunter auch bei der Deutschen Bahn und in britischen Krankenhäusern. Bei den Schadprogrammen im Umlauf registrierte das BSI eine kräftige Zunahme: Die Zahl stieg von mehr als 600 Millionen im Jahr 2017 auf mehr als 800 Millionen 2018. Die Zahl der Schadprogramm-Varianten pro Tag sei von 280.000 auf 390.000 gestiegen. Der Bericht deckt den Zeitraum vom 1. Juli 2017 bis zum 31. Mai 2018 ab.

Neue Angriffsziele entstehen mit der zunehmenden Vernetzung von Alltagsgegenständen wie Stromzählern, Heizungen oder auch Medizinprodukten. So sei es unter Laborbedingungen etwa gelungen, Herzschrittmacher oder Beatmungsgeräte zu hacken und umzuprogrammieren, schreibt das BSI in seinem Bericht. Gleichzeitig werde gerade bei solchen Geräten auf eine bessere Verschlüsselung verzichtet, etwa um Ärzten im Notfall einen raschen Zugriff zu ermöglichen. Da die Gefährdungslage kritisch sei, müsse noch stärker an speziellen Sicherheitsmechanismen geforscht werden.

Grüne fordern IT-Sicherheitsgesetz

Die Grünen werfen der Bundesregierung derweil Nachlässigkeit bei der IT-Sicherheitspolitik vor. „Derzeit erreichen uns täglich Meldungen über verheerende Datenskandale und geheimdienstliche Versuche, digitale Infrastrukturen und private Kommunikation zu kompromittieren", sagte der Vize-Fraktionschef der Grünen, Konstantin von Notz. „Die Einschläge kommen täglich näher und die Gefahr eines neuen Kriegsschauplatzes im Digitalen ist durchaus real."

Freitag, 28. September 2018

50 Millionen Profile betroffen

Facebook meldet Hackerattacke

Facebook erlaubt Nutzern, ihr eigenes Profil zu betrachten. Über diese Funktion aber schlichen Angreifer ins soziale Netzwerk. Inzwischen ist die Lücke wieder verschlossen, das genaue Ausmaß des Angriffs aber noch unklar.

Ein halbes Jahr nach dem Facebook-Datenskandal um Cambridge Analytica stellt nun ein massiver Hacker-Angriff das Vertrauen der Nutzer auf die Probe. Fast 50 Millionen Mitglieder des weltgrößten Online-Netzwerks sind direkt betroffen. Die Angreifer hätten digitale Schlüssel zu ihren Accounts gestohlen, mit denen sie „die Profile nutzen konnten als seien es ihre eigenen", sagte Facebook-Manager Guy Rosen.

Nach bisherigen Erkenntnissen hätten die Hacker aber keine privaten Nachrichten abgerufen oder versucht, etwas im Namen der betroffenen Nutzer bei Facebook zu posten, hieß es. Zugleich hätten die Angreifer aber in großem Stil Profil-Informationen wie Name, Geschlecht und Wohnort abgerufen. Dadurch sei die Attacke auch aufgefallen. Bisher habe Facebook keinen Fokus auf bestimmte Regionen oder Nutzergruppen feststellen können.

Erschwerend kommt hinzu, dass die Angreifer sich mit den erbeuteten Digitalschlüsseln auch bei anderen Online-Diensten anmelden konnten, die mit dem Facebook-Login genutzt wurden. Ob es dazu kam, ist bisher unklar. Die Sicherheitslücke sei am Donnerstag geschlossen worden, betonte Facebook.

Auch Zuckerbergs Profil betroffen

Zumindest gemessen an der Zahl betroffener Nutzer ist es der bisher größte Hacker-Angriff auf das Online-Netzwerk. „Wir wissen nicht, wer hinter dieser Attacke steckt", sagte Facebooks Gründer und Chef Mark Zuckerberg in einer eilig einberufenen Telefonkonferenz. Man werde das möglicherweise auch nie erfahren, führte Produktchef Rosen hinzu. Auch die Profile von Zuckerberg und Geschäftsfuhrerin Sheryl Sandberg seien betroffen gewesen, berichteten die „New York Times" und die „Financial Times".

Die Angreifer hätten eine Sicherheitslücke in der Funktion ausgenutzt, mit der Facebook-Mitglieder sich ihr Profil aus der Sicht anderer Nutzer anzeigen lassen können, erläuterte das Unternehmen. Die Schwachstelle erlaubte es ihnen demnach, die sogenannten Token zu stehlen – eine Art Langzeitschlüssel, der auf einem Gerät gespeichert wird. Damit kann ein Nutzer schnell in sein Profil reinkommen, ohne jedes Mal ein Passwort eingeben zu müssen. Facebook stellte nach eigenen Angaben fest, dass rund 50 Millionen dieser Token gestohlen wurden. Das Passwort selbst ist dabei nicht betroffen.

Die Funktion mit der Anzeige des Profils aus Sicht von Dritten – mit der Nutzer eigentlich ihre Privatsphäre besser im Griff haben sollten – sei vorerst sicherheitshalber abgeschaltet worden, teilte Facebook weiter mit. Zur Sicherheit werden sich weitere rund 40 Millionen Nutzer auf ihren Geräten neu anmelden mussen, nur weil sie diese Funktion im vergangenen Jahr benutzt haben.

Behörden in Irland eingeschaltet

Facebook machte keine Angaben dazu, wann genau die Hacker die Token gestohlen und damit Zu-

griff auf die Nutzer-Profile gehabt haben könnten. Facebook habe zunächst ungewöhnlich hohe Aktivität bei einer Schnittstelle am 16. September entdeckt. Am Dienstagabend dieser Woche sei man dann sicher gewesen, dass eine Attacke laufe und habe die Sicherheitslücke bis Donnerstag gefunden und geschlossen. Neben dem FBI seien gemäß der EU-Datenschutzverordnung (DSGVO) auch Behörden in Irland eingeschaltet worden.

Facebook hat insgesamt mehr als zwei Milliarden aktive Mitglieder. Die Attacke kommt zu einem extrem ungünstigen Zeitpunkt für das Online-Netzwerk, das noch um das Vertrauen der Nutzer nach dem Datenskandal um Cambridge Analytica kämpfen muss. Die Datenanalyse-Firma hatte unberechtigterweise Zugang zu Informationen von Dutzenden Millionen Nutzern bekommen. Die Enthüllung dieses Vorgangs hatte Facebook in die bisher schwerste Krise gestürzt.

Zudem versucht Facebook gerade mit größten Anstrengungen, die Plattform vor den wichtigen Kongress-Wahlen in den USA im November gegen Manipulation von außen abzusichern. Die Facebook-Aktie fiel zum US-Handelsschluss um rund 2,6 Prozent.