Donnerstag, 19.12.2019

Hacker lassen grüßen

Weihnachtspost vom Trojaner-König Emotet

Sicherheitsbehörden warnen eindringlich vor einer neuen Angriffswelle des Trojaners Emotet. Die gefährlichste Schad-Software der Welt nutzt die Weihnachtszeit, um sich weiter zu verbreiten. Besonders betroffen sind Behörden, aber auch Unternehmen und andere Organisationen.

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) warnt vor einer neuen Angriffswelle des Trojaners Emotet. Offenbar hat es die Schad-Software aktuell vor allem auf Bundesbehörden abgesehen. Es seien „in den vergangenen Tagen mehrere bestätigte Emotet-Infektionen in Behörden der Bundesverwaltung gemeldet worden", schreibt das BSI. Dazu kämen weitere Verdachtsfälle.

Es handle sich um Erstinfektionen, die dazu führten, dass weitere Spam-Mails im Namen der Betroffenen verschickt werden, so das BSI. Man stehe mit den betroffenen Behörden in engem Kontakt, zu einer Schadauswirkung sei es bei ihnen bislang nicht gekommen, da die Infektionen isoliert und bereinigt werden konnten.

Unverdächtige Weihnachtsgrüße

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) schreibt, die Hacker verschickten unter anderem Weihnachtsgrüße von vermeintlich bekannten Kommunikationspartnern. Solche E-Mails gehen bei Unternehmen, Behörden und anderen Organisationen derzeit sehr häufig ein und werden routinemäßig behandelt. Genau das dürfen die Empfänger aber nicht tun, sie müssen in diesen Tagen besonders aufmerksam sein.

Sicherheitsbehörden haben in den vergangenen Monaten wiederholt vor Emotet gewarnt, das BSI nennt den Trojaner die „weltweit gefährlichste Schadsoftware". Unter anderem ist er so gefährlich, weil er ständig weiter verbessert wird und mit immer raffinierteren Methoden Nutzer dazu bringt, infizierte Anhänge zu öffnen.

Emotet hat die Fähigkeit, aus E-Mail-Programmen neben Kontaktinformationen und -beziehungen auch Nachrichteninhalte auszulesen. Damit täuschen die Angreifer sehr echt wirkende Antworten auf tatsächlich von einem Nutzer versandte E-Mails vor. Das macht die Spam-Mails besonders glaubwürdig und die Opfer öffnen infizierte Anhänge oder klicken auf Download-Links zu Office-Dokumenten, in denen die Schadsoftware in Form von Makros lauert. Auf den infizierten Systemen späht Emotet wiederum E-Mail-Konten und -Nachrichten aus und verwendet die Informationen seines Opfers, um sich weiterzuverbreiten.

Ein Trojaner kommt selten allein

Emotet nutzt befallene Computer aber nicht nur dazu, weitere Spam-Mails zu verschicken. Er lädt

weitere Schadsoftware nach. Normalerweise ist das zunächst ein Banking-Trojaner, der den Tätern den vollständigen Zugriff auf ein Netzwerk verschafft. So können die Angreifer unter anderem einen Erpresser-Trojaner einzusetzen, der Daten verschlüsselt oder ganze Netzwerke lahmlegt und dann Lösegeld fordert.

Sollte eine verdächtige Mail oder der entsprechende Anhang dennoch geöffnet worden sein, sollten Anwenderinnen und Anwender umgehend ihren IT-Sicherheitsbeauftragten informieren, rät das BSI und gibt konkrete Verhaltensempfehlungen:

Wie Sie sich schützen können:

- Installieren Sie zeitnah bereitgestellte Sicherheitsupdates für Betriebssysteme und Anwendungsprogramme (Web-Browser, E-Mail-Clients, Office-Anwendungen und so weiter).
- Setzen Sie Antiviren-Software ein und aktualisieren Sie diese immer wieder.
- Sichern Sie regelmäßig Ihre Daten (Backups).
- Richten Sie ein gesondertes Benutzerkonto auf dem Computer ein, um zu surfen und E-Mails zu schreiben.
- Öffnen Sie auch bei vermeintlich bekannten Absendern nur mit Vorsicht Dateianhänge von E-Mails (insbesondere Office-Dokumente) und prüfen Sie in den Nachrichten enthaltene Links, bevor Sie diese anklicken. Bei einer verdächtigen E-Mail sollten Sie im Zweifelsfall den Absender anrufen und sich nach der Glaubhaftigkeit des Inhaltes erkundigen.

Was Sie tun können, wenn Sie betroffen sind:

- Informieren Sie Ihr Umfeld über die Infektion, denn Ihre Mailkontakte sind in diesem Fall besonders gefährdet.
- Ändern Sie alle auf den betroffenen Systemen (zum Beispiel im Web-Browser) gespeicherten und eingegebenen Zugangsdaten.
- Die Schadprogramme nehmen teilweise tiefgreifende (sicherheitsrelevante) Änderungen am infizierten System vor. Sollte Ihr Rechner mit Schadsoftware wie Emotet infiziert sein, dann empfiehlt das BSI, diesen Rechner neu aufzusetzen.

Donnerstag, 14.11.2019

Cyberangriff auf Erdölkonzern

Hacker fordern Lösegeld von Pemex

Die Deutsche Bahn, Beiersdorf, Maersk oder auch Renault hat es in der Vergangenheit bereits getroffen: Hacker griffen die Computersysteme der Konzerne an, forderten zum Teil hohe Lösegelder. Nun wird der Erdölriese Pemex attackiert.

Nach einem Cyberangriff auf den mexikanischen Erdölkonzern Pemex sieht sich das Unternehmen einem Erpressungsversuch ausgesetzt. Pemex sei ein seriöser Konzern und werde daher nicht zahlen, sagte Mexikos Energieministerin Rocío Nahle. Nach Medienberichten hatte ein Hacker Lösegeld in Höhe von 565 Bitcoin – umgerechnet rund 4,5 Millionen Euro – verlangt, um Daten, die beim Cyberangriff vom vergangenen Sonntag verschlüsselt wurden, wieder zu entschlüsseln.

Pemex hatte mitgeteilt, dass versuchte Cyberangriffe „neutralisiert" worden seien. Das Funktionieren von mindestens fünf Prozent der Computer des Unternehmens sei betroffen. Der Betrieb laufe aber normal weiter und der Benzinbestand sei gesichert, hieß es.

Pemex ist einer der am stärksten verschuldeten Energiekonzerne der Welt. Die Verbindlichkeiten belaufen sich trotz Hilfen der mexikanischen Regierung derzeit auf knapp 100 Milliarden US-Dollar.

Cyberattacken mit Erpressungs-Trojanern hatten in der Vergangenheit bereits mehrfach für Schlagzeilen gesorgt. So gab es im Mai und im Juni 2017 zwei große Angriffswellen, bei denen unter anderem der Nivea-Hersteller Beiersdorf, die dänische Reederei Maersk, der Autobauer Renault, Krankenhäuser in Großbritannien und die Deutsche Bahn betroffen waren.

Donnerstag, 17.10.2019

Hacker agieren wie Geheimdienste

BSI registriert täglich 450.000 Attacken

Die Zahl der Cyberangriffe mit schädlicher Software nimmt rasant zu. Doch nicht nur die Quantität nimmt laut Bundesamt für Sicherheit in der Informationstechnik zu. Hacker werden immer professioneller und erinnern bei ihrem Vorgehen an staatliche Geheimdienste.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Berlin hat bei der Vorstellung des jährlichen Lageberichts vor einer neuen Qualität der Cyber-Bedrohung gewarnt. Die Zahl der Schadsoftwares sei auf 900 Millionen angestiegen, allein im September von 300.000 auf 450.000 täglich, sagte BSI-Präsident Arne Schönbohm.

Cyberkriminelle würden immer häufiger Techniken einsetzen, die „bisher nur bei Advanced Persistent Threats (APTs) eingesetzt werden". Unter APT werden Hackergruppen zusammengefasst, hinter denen staatliche Akteure vermutet werden, so wie der russische Geheimdienst GRU. Das Angriffsniveau sei laut Schönbohm so hoch wie bei Nachrichtendiensten. „Das BSI rechnet künftig mit einer weiteren Zunahme an gut umgesetzten, automatisierten Social-Engineering-Angriffen dieser Art, die für die Empfänger kaum noch als solche zu identifizieren sind."

Als „König der Schadsoftwares" nannte Schönbohm das Programm Emotet. Die bereits seit 2010 bekannte Malware sei seit November 2018 wieder vermehrt mithilfe schädlicher Office-Dokumente verteilt worden, heißt es in dem Bericht. Emotet habe „vor allem in der Wirtschaft teils erhebliche Schäden angerichtet", sagte Schönbohm, und bleibe dort auch weiterhin eine Gefahr. Auch komme es vermehrt zu Attacken durch Ransomware, Bot-Infektionen und Identitätsdiebstähle.

Angesichts der anhaltend hohen Bedrohung durch Cyber-Angriffe will Bundesinnenminister Horst Seehofer die Befugnisse der Sicherheitsbehörden ausweiten. „Wir brauchen ein Internet-Sicherheitsgesetz 2.0", sagte Seehofer anlässlich der Vorstellung des Lageberichts des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Berlin. Dazu sei er mit Justizministerin Christine Lambrecht (SPD) in Kontakt. „Das läuft recht gut." Er sei überzeugt, „dass wir da auch dieses Gesetz bekommen". Mit dem Entwurf soll das BSI nicht nur defensiv schützen, sondern auch in IT-Systeme eindringen.

Mittwoch, 16.10.2019

Über 200 Server ausgefallen

IT-Störung legt Porsche-Produktion lahm

Eine IT-Störung hat fuür einen Produktions-Stopp bei Porsche gesorgt. Betroffen waren die Werke in Stuttgart-Zuffenhausen und Leipzig. Es soll sich dabei aber nicht um einen Hacker-Angriff handeln.

Eine IT-Störung hat am gestrigen Dienstag für einige Stunden die Produktion beim Sportwagenbauer Porsche lahmgelegt. Betroffen waren das Stammwerk in Stuttgart-Zuffenhausen sowie das Werk in Leipzig, wie ein Sprecher sagte. Zuvor hatte „Spiegel Online“ berichtet. Es habe sich um ein internes Problem gehandelt, das sich auf Produktion und Logistik an den beiden Standorten ausgewirkt habe, und nicht um einen Angriff von außen, betonte der Sprecher. Mehr als 200 Server seien ausgefallen, die Produktion sei jedoch am Abend wieder angelaufen.

Porsche produziert in seinem Stammwerk die zweitürigen Sportwagen 911 und 718 sowie neuerdings das Elektromodell Taycan. In Leipzig werden der kleine SUV Macan und der viertürige Panamera gebaut. Wie groß die Auswirkungen der Störung auf die Produktion waren, konnte der Sprecher noch nicht exakt beziffern.

Mittwoch, 25.09.2019

BSI warnt eindringlich

Trojaner-König Emotet greift massiv an

Das BSI warnt erneut eindringlich vor der extrem gefährlichen Schadsoftware Emotet. Der Trojaner wird seit einigen Tagen über E-Mails massenhaft versandt und hat bereits große Schäden angerichtet. Nutzer müssen darauf vorbereitet sein, selbst zum Ziel zu werden.

Das Bundesamt fur Sicherheit in der Informationstechnologie (BSI) nennt Emotet die „weltweit gefährlichste Schadsoftware" und hat schon mehrmals vor dem Trojaner gewarnt. Unter anderem ist er so gefährlich, weil er ständig weiter verbessert wird und mit immer raffinierteren Methoden Nutzer dazu bringt, infizierte Anhänge zu öffnen. Jetzt schlägt das BSI erneut Alarm, weil eine neue, massive Angriffswelle rollt, die „in den vergangenen Tagen erhebliche Schäden in der deutschen Wirtschaft, aber auch bei Behörden und Organisationen verursacht" hat.

„Seit rund einer Woche wird Emotet wieder massenhaft versandt und hat binnen weniger Tage fur Produktionsausfälle, den Ausfall von Burgerdiensten in Kommunalverwaltungen und zahlreiche infizierte Netzwerke gesorgt", schreibt BSI-Chef Arne Schönbohm. Aber auch Privatanwender stunden im Fokus der Angreifer, da Emotet weitere Schadsoftware nachlade, die zu Angriffen auf das Online-Banking eingesetzt werden könnten.

Emotet täuscht und erpresst

Emotet hat die Fähigkeit, aus E-Mail-Programmen neben Kontaktinformationen und -beziehungen auch Nachrichteninhalte auslesen zu können. Damit täuschen die Angreifer sehr echt wirkende Antworten auf tatsächlich von einem Nutzer versandte E-Mails vor. Das macht die Spam-Mails besonders glaubwurdig und die Opfer öffnen infizierte Anhänge oder klicken auf Download-Links zu Office-Dokumenten, in denen die Schadsoftware in Form von Makros lauert. Auf den infizierten Systemen spät Emotet wiederum E-Mail-Konten und -Nachrichten aus und verwendet die Informationen seines Opfers, um sich weiterzuverbreiten.

Emotet nutzt befallene Computer aber nicht nur dazu aus, weitere Spam-Mails zu verschicken. Er lädt weitere Schadsoftware nach. Normalerweise ist das zunächst ein Banking-Trojaner, der den Tätern den vollständigen Zugriff auf ein Netzwerk verschafft. So können die Angreifer unter anderem einen Erpresser-Trojaner einzusetzen, der Daten verschlusselt oder ganze Netzwerke lahmlegt und dann Lösegeld fordert.

Mehrere tausend Infektionen in wenigen Tagen

In den vergangenen Tagen habe man mehrere tausend E-Mail-Konten von Unternehmen und Burgern, die durch eine Infektion mit Emotet kompromittiert und anschließend fur den Spam-Versand missbraucht wurden, an die jeweils zuständigen Provider gemeldet, schreibt das BSI. Die Provider seien gebeten worden, die Sensibilisierung der Belegschaft genauso wie regelmäßige Backups oder das Einspielen von Sicherheitsupdates. Genauere Anweisungen gibt das BSI auf der Webseite „Maßnahmen zum Schutz vor Emotet und gefährlichen E-Mails im Allgemeinen".

Montag, 09.09.2019

Viele surfen ohne Virenschutz

Jeder Vierte von Cyberkriminalität betroffen

Schadsoftware, Viren oder sogenannte Trojaner: Fast jeder vierte Internetnutzer hat Erfahrungen mit Angriffen aus dem Netz. Die Polizei geht von einer hohen Dunkelziffer aus, da nur jedes dritte Cyberverbrechen gemeldet wird. Besonders jungere Menschen sind demnach anfällig fur Cyberattacken.

Knapp jeder vierte Internetnutzer in Deutschland (24 Prozent) ist schon mindestens einmal Opfer von Cyberkriminalität geworden. Besonders häufig trifft es jungere Menschen. Wie eine aktuelle repräsentative Studie vom Bundesamt fur Sicherheit in der Informationstechnik (BSI) zeigt, haben 36 Prozent der Betroffenen Betrug beim Onlineshopping erlebt. Bei 28 Prozent von ihnen wurden vertrauliche Daten abgefischt, 26 Prozent der Betroffenen berichteten von Schadsoftware-Angriffen durch Viren oder sogenannte Trojaner. In 18 Prozent der Fälle ging es um Identitätsdiebstahl. Mit Cybermobbing oder Erpressersoftware haben jeweils 13 Prozent der Betroffenen Erfahrungen gemacht.

Das „Digitalbarometer" wird einmal jährlich zusammen mit dem Programm Polizeiliche Kriminalprävention der Länder und des Bundes erstellt, um Probleme im Bereich der Cyber- Sicherheit zu identifizieren. Zu diesen Problemen zählt nicht nur die Nachlässigkeit vieler Nutzer, wenn es um den Schutz vor Online-Angriffen geht. Auch den Zugang zu Informationen uber aktuelle Bedrohungen empfinden viele Burger laut Studie als nicht optimal.

Über ein Drittel surft ohne Antivirenprogramm

Den Angaben zufolge haben nur 61 Prozent der Menschen, die online gehen, Antivirenprogramme installiert. Lediglich 58 Prozent der Befragten gaben an, sichere Passwörter zu nutzen. Mehr als 60 Prozent der Nutzer installieren Updates nicht sofort. Seine E-Mails verschlusselt immerhin knapp jeder Funfte (19 Prozent).

Dass jungere Menschen wesentlich häufiger Opfer von Internet-Kriminalität werden als Ältere, hat laut Studie nicht nur damit zu tun, dass sie mehr Dinge online erledigen – vom Fahrkartenkauf bis zur Interaktion via Social Media. Ein weiterer Grund durfte sein, dass sie sorgloser sind, was Straftaten im Internet angeht. Während fast die Hälfte (49 Prozent) der 60- bis 66-Jährigen Empfehlungen zur Erhöhung der Sicherheit sofort umsetzt, tut dies von den 16- bis 29-Jährigen nur etwa jeder Vierte (26 Prozent).

Positiv beurteilte BSI-Vizepräsident Gerhard Schabhuser bei der Vorstellung der Studie am Montag in Berlin die Entwicklung beim Online-Banking. Hier habe die Zwei-Faktor-Authentifizierung zu einer deutlichen Verbesserung gefuhrt. Neben einem Passwort wird dabei immer noch ein zweiter Sicherheitsfaktor eingebaut – etwa ein Fingerabdruck oder eine uber einen Tan-Generator generierte Nummer.

Polizei sieht hohe Dunkelziffer

Von den meisten Cyberangriffen erfährt die Polizei nichts. Denn das „Digitalbarometer 2019" zeigt: Nur jeder dritte Fall wird angezeigt. Die Aufklärungsquote lag zuletzt bei knapp 38 Prozent. Fur das vergangene Jahr weist die Polizeiliche Kriminalstatistik rund 272.000 Straftaten „mit Tatmittel Inter-

Samstag, 07.09.2019

„Massive" Attacke im Netz

Angreifer legen Wikipedia lahm

Eine der beliebtesten Internetseiten Deutschlands ist vorübergehend nicht zu erreichen: Mit einem gezielten Angriff zwingen bislang unbekannte Täter die Server von Wikimedia in die Knie. Bei Twitter brüsten sich die Angreifer mit ihren Fähigkeiten.

Die deutsche Version des Online-Lexikons Wikipedia und einige andere Ausgaben in Europa sind in der Nacht auf Samstag Ziel einer umfangreichen Online-Attacke geworden. Die Betreibergesellschaft Wikimedia Deutschland berichtete von einem sogenannten DDOS-Angriff.

Bei solchen Attacken fluten Angreifer die Server ihrer Opfer mit Unmengen sinnloser Anfragen, bis die Kapazitätsgrenzen erreicht sind und die Systeme ausfallen. Betreiber größerer Internetangebote versuchen sich in der Regel mit speziellen Abwehrmechanismen vor solchen Attacken zu schützen.

Bei Wikimedia war von einem „massiven und sehr breit angelegten" Angriff die Rede. Kurz vor Mitternacht ließen sich die Wikipedia-Seiten kurzzeitig wieder aufrufen, bevor wieder nichts ging. Auch Nutzer unter anderem in Großbritannien und Frankreich meldeten Probleme.

„UKDrillas" triumphiert auf Twitter

Bei Twitter tauchte eine Art Bekennerschreiben auf: Per frisch eingerichtetem Account verkündete eine bislang unbekannte Gruppierung namens „UKDrillas", sie stecke hinter dem Angriff. Um diese Behauptung zu belegen, verkündeten sie kurz vor Mitternacht, die Attacke für kurze Zeit auszusetzen, bevor sie wieder hochgefahren werde. In diesem Zeitraum war die Online-Enzyklopädie dann tatsächlich erreichbar.

Der oder die Täter veröffentlichten im Netz technische Details zum Angriff wie etwa einzelne IP-Adressen und brüsteten sich mit ihrer Tat. Der Angriff auf die beliebte Netz-Enzyklopädie diente demnach nur zur Übung. Mehrfach bestätigten die Twitter-Nutzer hinter „UKDrillas", dass sie nur einen begrenzten Angriff fahren wollten, um neue Techniken zu nutzen. Wiederholt gingen der oder die Täter auch auf Anfragen oder Kommentare anderer Twitter- Nutzer ein. Sie wollten damit „einige neue Dinge" ausprobieren, hieß es. Die Attacke werde nach einigen Stunden gestoppt.

Mittwoch, 21.08.2019

Studie zu Cyber-Attacken

Unternehmen leiden massiv unter Hackern

Das Internet ist ein zunehmend gefährlicher Raum. Eine Studie kommt zu dem Ergebnis, dass die Gefahren fur die deutsche Wirtschaft, Gesellschaft und Politik durch Angriffe aus dem Cyber-Space weiter gestiegen sind. Viele Unternehmen berichten inzwischen von täglichen Attacken.

Die große Mehrheit der deutschen Unternehmen hat bereits schmerzhafte Erfahrungen mit Internetgefahren gesammelt. 85 Prozent aller mittleren und großen Unternehmen in Deutschland sehen sich Cyber-Angriffen ausgesetzt. Das ist das Ergebnis einer Studie des Instituts fur Demoskopie Allensbach im Auftrag der Wirtschaftsprufungsgesellschaft Deloitte. 28 Prozent der Firmen berichten demnach von täglichen Angriffen, bei weiteren 19 Prozent kommt das mindestens einmal wöchentlich vor.

Besonders häufig haben große Unternehmen mit Cyber-Attacken zu tun – Firmen mit 1000 und mehr Mitarbeitern zu 40 Prozent täglich. Die Frequenz der Angriffe hat laut Cyber Security Report im Vergleich zu den Vorjahren zugenommen. Bei rund jedem funften Unternehmen haben solche Angriffe bereits spurbare – in einigen Fällen sogar massive – Schäden verursacht, heißt es in dem Bericht.

Neben Angriffen auf die IT-Systeme erwachsen Unternehmen auch aus den sozialen Netzwerken diverse Bedrohungen. Bei rund einem Viertel berichten Unternehmen von Versuchen, den Ruf der Firma durch gezielte Falschinformationen im Internet zu schädigen. Dennoch verfolgt nur rund die Hälfte systematisch, was in sozialen Netzwerken uber ihre Organisation geäußert wird.

Fake News an der Spitze des Risiko-Rankings

Fur den Bericht zu Cyber-Risiken und IT-Sicherheit befragte das Institut fur Demoskopie Allensbach Hunderte von Fuhrungskräften aus großen und mittleren Unternehmen sowie Abgeordnete des Bundestags, der Landtage und des Europaparlaments. Sowohl Abgeordnete als auch Unternehmen setzten Fake News an die Spitze ihres Risiko-Rankings. „Soziale Medien verändern das Informationsverhalten und den politischen Diskurs gravierend. Die Tragweite dieser Entwicklung wird bisher nicht annähernd erkannt. Die Besorgnis vieler Abgeordneter ist durchaus verständlich“, sagte Renate Köcher, Geschäftsfuhrerin des Instituts fur Demoskopie Allensbach.

Zugleich schätzten Unternehmen viele Gefahren höher ein als die Abgeordneten. So furchten sich 73 Prozent der befragten Unternehmer und lediglich 58 Prozent der Politiker vor Datenbetrug im Internet. Eingriffe in die Privatsphäre von Burgern durch vernetzte Haustechnik bewerteten 55 Prozent der Unternehmer und 43 Prozent der Politiker als wachsendes Sicherheitsrisiko.

Einig sind sich Wirtschaftsfuhrer und Abgeordnete in der Auffassung, dass die Politik zur Bekämpfung von Cyber-Risiken in Unternehmen beitragen kann. 90 Prozent der Unternehmensvertreter waren dieser Ansicht, Politiker stimmten zu 100 Prozent zu. Da gleichzeitig lediglich neun Prozent der Manager mit staatlichen Einrichtungen im Bereich der Cyber-Sicherheit vertraut sind, empfehlen die Autoren der Studie einen stärkeren Austausch in dem Bereich.

net“ aus – acht Prozent mehr als 2017. „Wir vermuten, dass es ein großes Dunkelfeld gibt“, sagte Martin von Simson, Referatsleiter im Bundesinnenministerium. Das liegt einerseits daran, dass manche Opfer den Aufwand einer Anzeige scheuen, weil sie keine große Summe Geld verloren haben oder aus Scham.

Denn neben Erpressungen im Stil von „Wir wissen, dass Du auf Porno-Seiten unterwegs bist“ gibt es auch Betruger, die online eine „Beziehung“ aufbauen, um dann anschließend in einer angeblichen Notlage Geld zu fordern. Typische Szenarien dabei sind die imaginäre junge hubsche Frau aus Russland oder der Ukraine, die sich Geld fur ihren Besuch bei einem älteren Mann in Deutschland schicken lässt, der dann aber nie stattfindet. Einsame Frauen im mittleren Alter fallen eher auf die Geschichte des vermeintlichen Ingenieurs herein, der in Afrika arbeitet und dort zum Beispiel einen Autounfall hat.

Mittwoch, 14.08.2019

Digitale Turschlösser unsicher

Hacker entdecken Mega-Datenleck im Web

Ein Fingerabdruck und schon öffnet sich die Tür zum Büro: Neben Firmen nutzen auch die britische Polizei und Banken „Biostar 2" als digitales Schloss. Doch zwei Hacker entdecken bei dem biometrischen Zutrittskontrollsystem jetzt eine gravierende Sicherheitslücke – auch wegen „lächerlich einfacher Passwörter".

Sicherheitsforscher aus Israel haben eine riesige Datenbank mit rund einer Million Fingerabdrücken und anderen biometrischen Daten aufgespürt, die quasi ungeschützt und unverschlüsselt im Web abgerufen werden konnte. Die Daten stammen Berichten des britischen „Guardians" sowie des israelischen Portals „Calacalist" zufolge vom System „Biostar 2" der koreanischen Sicherheitsfirma Suprema, die nach eigenen Angaben Marktführer in Europa bei biometrischen Zutrittskontrollsystemen ist.

„Biostar 2" arbeitet mit Fingerabdrücken oder Gesichtsscans auf einer webbasierten Plattform für intelligente Türschlösser, mit der Unternehmen die Zugangskontrolle für ihre Büros oder Lagerhallen selbst organisieren können. Das System wird nach Angaben des „Guardians" auch von der britischen Polizei sowie mehreren Verteidigungsunternehmen und Banken genutzt.

Die gravierende Sicherheitslücke wurde von den israelischen Hackern Noam Rotem und Ran Lokar entdeckt, die für den Dienst vpnMentor arbeiten. Die Schwachstelle habe dazu geführt, dass man die vollständige Kontrolle über die Konten im System erhalten konnte, sagte Rotem dem Portal „Calcalist".

Leichtfertige Absicherung mit „abcd1234"

Den Berichten zufolge hatten die Forscher Zugriff auf mehr als 27,8 Millionen Datensätze und 23 Gigabyte Daten, darunter Fingerabdruck- und Gesichtserkennungsdaten, Gesichtsfotos von Benutzern, unverschlüsselte Benutzernamen und Passwörter, Protokolle über den Zugang zu den Einrichtungen, Sicherheitsstufen und -freigabe sowie persönliche Daten des Personals. Außerdem hätten sie Datensätze in den Firmenkonten neu anlegen und manipulieren können.

Entsetzt zeigten sich die Forscher darüber, dass in dem System die vollständigen biometrischen Daten meist unverschlüsselt abgespeichert wurden. „Anstatt einen Hash des Fingerabdrucks zu speichern, der nicht rückentwickelt werden kann, speichern sie die tatsächlichen Fingerabdrücke der Menschen, die für bösartige Zwecke kopiert werden können", sagten die Forscher dem „Guardian". Überrascht waren Rotem und Lokar darüber, wie schlecht die Suprema-Kunden zum Teil ihre Konten abgesichert haben: „Viele Konten enthielten lächerlich einfache Passwörter wie ‚Passwort' und ‚abcd1234'".

Der Marketingleiter von Suprema, Andy Ahn, sagte, das Unternehmen habe eine „eingehende Bewertung" der von vpnMentor bereitgestellten Informationen vorgenommen. Die Kunden wurden im Falle einer Bedrohung informiert. Die Sicherheitslücke sei inzwischen geschlossen worden.

Dienstag, 25.07.2019

Anrufprotokolle erbeutet

Hacker knacken weltweit Mobilfunkanbieter

Eine Sicherheitsfirma deckt auf, dass Cyberkriminelle weltweit Mobilfunkanbieter angegriffen und Anrufprotokolle und andere Nutzerdaten geklaut haben. Die Spur führt nach China zu einer weltweit berüchtigten Hackergruppe.

Die US-Sicherheitsfirma Cybereason deckt auf, dass Hacker weltweit mehr als zehn Firmennetzwerke von Mobilfunkanbietern geknackt und dabei Zugriff auf Zugangsdaten, Rechnungen und Anrufprotokollen von vielen Millionen Nutzern erhalten haben. Letztendlich hätten die Angreifer die komplette Kontrolle uber die Netzwerke erhalten können, schreiben die Sicherheitsforscher. Die Hacker waren aber nicht daran interessiert, massenhaft Informationen abzugreifen, sondern gingen gezielt gegen mindestens 20 Einzelpersonen vor.

Anrufprotokolle enthalten unter anderem Datum, Uhrzeit, Ort, Ziel und Dauer eines Gesprächs sowie Informationen über die genutzten Geräte. Auch ohne Gesprächsinhalte sind solche Metadaten extrem wertvoll vor allem für Ermittlungsbehörden und Geheimdienste, da die Informationen sehr viel über eine Person verraten.

Alles deutet auf China hin

Auch die ausgeklügelte und hochprofessionelle Vorgehensweise der „Operation Soft Cell" spricht laut Cybereason für eine staatliche Organisation. Werkzeuge, Techniken und Motive deuteten sehr klar auf die berüchtigte Hackergruppe APT10 hin, die im Auftrag Pekings tätig ist. Außerdem hätten alle ausspionierten Personen Verbindungen mit China. Allerdings sei es auch möglich, dass andere Angreifer APT10 imitieren, um eine falsche Fährte zu legen. Dies sei aber eher unwahrscheinlich, schreiben die Sicherheitsforscher.

„Operation Soft Cell" soll mindestens seit 2017 laufen, wobei es Hinweise gebe, dass die Aktion schon früher begonnen habe. Welche Mobilfunkanbieter gehackt wurden, teilt Cybereason nicht mit. Sie befänden in sich in Europa, Asien, Afrika und Nahost. Es sollen einige sehr große Unternehmen darunter sein, aber auch kleinere Anbieter an speziellen Orten. US-Provider sollen bisher nicht betroffen sein.

APT10 stand unter anderem im vergangenen Dezember bei einem Prozess gegen zwei mutmaßliche Mitglieder der Hackergruppe im Rampenlicht. Sie sollen an großangelegten Angriffen auf die USA und ihre Verbündeten massenhaft Daten bei Firmen und Behörden gestohlen haben. Computer in mindestens einem Dutzend Länder sollen dabei gehackt worden sein, um „Chinas Geheimdienst Zugang zu sensiblen Unternehmensinformationen zu verschaffen", sagte der stellvertretende US-Justizminister Rod Rosenstein.

Dienstag, 02.07.2019

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-Sicher- heit 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 Hauptaugenmerk 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 Cyber- crime 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 Da-

teien 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, 12.02.2019

Erneut Hunderte Millionen Nutzerkonten im Darknet

Schon wieder bieten Hacker im Darknet einen gewaltigen Datensatz mit Hunderten Millionen geklauten E-Mail- Adressen und Passwörtern an. Sie stammen von 16 verschiedenen Websites, von denen einige sehr viele Nutzer haben.

Wenige Wochen nachdem Sicherheitsforscher auf einen zig Gigabyte großen Datensatz mit Log-in-Informationen stießen, werden erneut viele Millionen Namen, E-Mail-Adressen und die zugehörigen Passwörter im Tor-Netzwerk (Darknet) angeboten. Laut „The Register" sind es rund 617 Millionen Internet-Konten, fur die der Verkäufer etwas weniger als 20.000 Dollar in Bitcoin haben möchte. Stichproben hätten ergeben, dass die Daten echt sind.

Sie wurden bei insgesamt 16 Websites erbeutet, was diesen Monster-Leak von „Collection #1" unterscheidet, bei dem E-Mail- Adressen und Passwörter aus sehr vielen Quellen stammen. Unter den gelisteten Websites befinden sich einige, die sehr populär sind und Millionen Nutzer haben. Die größte gehackte Website ist Dubsmash mit 162 Millionen, die kleinste DataCamp mit 700.000 Nutzern.

Außerdem betroffen: MyFitnessPal (151 Millionen), MyHeritage (92 Millionen), ShareThis (41 Millionen), HauteLook (28 Millionen), Animoto (Millionen), EyeEm (Millionen), 8fit (20 Millionen), Whitepages (18 Millionen), Fotolog (16 Millionen), 500px (15 Millionen), Armor Games (11 Millionen), BookMate (8 Millionen), CoffeeMeetsBagel (6 Millionen), Artsy (1 Million).

„Ich brauche das Geld"

„Heise" schreibt, einige Hacks seien schon bekannt gewesen, beispielsweise von MyFitness. Andere Websites wie die Fotografie-Community 500px hätten bisher nicht gewusst, dass bei ihnen Daten abgegriffen wurden.

Der Verkäufer sagte „The Register", seine Gruppe sei insgesamt im Besitz von rund einer Milliarde Datensätze, die sie seit 2012 erbeutet hätten. Nicht alle stunden zum Verkauf, einige wurden „privat" genutzt. Er sei kein wirklich böser Mensch, aber er brauche das Geld und wolle, dass die Leaks offengelegt werden.

Auch wenn er sich nicht fur sehr böse hält, können die von ihm verkauften Daten doch großen Schaden anrichten. Zwar lägen die Passwörter nicht im Klartext vor, aber die Verschlusselung sei teilweise veraltet und relativ leicht zu knacken, schreibt „The Register". „Heise" ergänzt, dass Angreifer erbeutete E-Mail-Adressen-Passwort-Paare bei vielen verschiedenen Online-Diensten ausprobieren, da Nutzer die Kombinationen oft mehrmals verwendeten.

Freitag, 01.02.2019

Ändere-dein-Passwort-Tag ist Unsinn

Der 1. Februar ist Ändere-dein-Passwort-Tag. Vielleicht hat dieses Motto früher einmal Sinn ergeben, doch heute ist es so dusselig wie ein Wechsle-deine-Unterhose-Tag. Das heißt nicht, dass man die Sicherheit seiner Online-Konten nicht ernst nehmen soll. Aber es gibt Wichtigeres zu tun.

Es war sicher gut gemeint, als 2012 der Ändere-dein-Passwort-Tag ins Leben gerufen wurde. Doch inzwischen hat sich die Welt weitergedreht und das Motto hat seinen Sinn verloren. Welcher Nutzer hat denn heutzutage nur noch ein Passwort? Wenn schon, dass müsste es Ändere-deine-Passwörter-Tag heißen. Doch auch so ein jährlich durchgeführtes Wechselspiel würde das Ziel, die Internet-Sicherheit von Nutzern zu erhöhen, weit verfehlen. Um das zu erreichen, gibt es weit wichtigere Dinge zu tun – und nicht nur vom Nutzer.

Gute Passwörter ändern nutzt nichts

Natürlich darf ein Passwort nicht leicht zu erraten sein, so viel sollte inzwischen allen klar sein. Der 1. Februar ist aber auch nicht der Erstelle-ein-sicheres-Passwort-Tag, man soll es ändern. Wenn man aber bereits gute Kombinationen verwendet, bringt es nicht viel, wenn man sie jährlich wechselt. Viel wichtiger ist, dass man für jeden Zugang ein eigenes sicheres Passwort verwendet und nicht für alle Online-Konten dasselbe. Denn so haben Hacker durch einen erfolgreichen Angriff Zugriff auf alle Logins eines Opfers. Und dann ist es auch völlig Wurst, ob das erbeutete Passwort kürzlich geändert wurde.

Sogenannte Brute-Force-Angriffe, bei denen Hacker versuchen, mit maschineller Hilfe Passwörter zu erraten, sind durch lange und möglichst sinnlose Kombinationen mit Sonderzeichen, Buchstaben, Zahlen und Groß- und Kleinschreibung gut abzuwehren. Das gilt vor allem bei wahllos durchgeführten Angriffen, die kein spezielles Ziel haben.

Anbieter sind in der Pflicht

Der kürzlich entdeckte Monster-Leak von hunderten Millionen E-Mail-Adressen und Passwörtern hat gezeigt, dass Zugangsdaten Hackern praktisch ausschließlich bei Angriffen auf Dienste und Websites in die Hände fallen. Und das liegt ausschließlich in der Verantwortung der Anbieter. Nutzer können ihre Passwörter so oft ändern wie sie wollen, wenn sie von Yahoo, Adobe, Linkedin & Co. nicht ausreichend geschützt werden. Die Sicherheit von Online-Konten ist tatsächlich nur zu einem sehr geringen Teil vom Nutzerverhalten abhängig. Trotzdem kann man etwas tun.

Wie bereits erwähnt, ist es besonders wichtig, für jeden Dienst ein individuelles Passwort zu verwenden. Damit dies bei vielen Konten und nötigerweise langen, komplizierten Kombinationen leichterfällt, empfiehlt es sich, einen Passwort-Manager zu verwenden. Er speichert gut abgesichert alle Zugangsdaten. Um sie abzurufen, muss man sich nur ein Master-Passwort merken.

Donnerstag, 17.01.2019

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.

Dienstag, 08.01.2019

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, 11.10.2018

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, 28.09.2018

50 Millionen Profile betroffen – Facebook meldet Hacker-attacke

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.

Donnerstag, 27.09.2018

Cyberkriminalität nimmt zu

Hacker verursachen millionenhohe Schäden

Die Schadsoftware „WannaCry" zählt nur zu den prominentesten Fällen: Angreifer legten damit bundesweit etwa Ticketschalter und Anzeigetafeln an Bahnhöfen lahm. Doch das ist kein Einzelfall. Die Kriminalität im Netz nimmt sogar noch zu.

Durch Computerbetrug sind in Deutschland im vergangenen Jahr Schäden in Höhe von mehr als 70 Millionen Euro entstanden. Das sind rund 20 Millionen Euro mehr als im Jahr davor, wie das Bundeskriminalamt (BKA) mitteilte. Insgesamt registrierte die Polizei 2017 rund 86.000 Fälle von Cyberkriminalität, was einem Anstieg um vier Prozent entspricht. Ein Beispiel war die Erpressersoftware „WannaCry", die im Mai 2017 Hunderttausende Computersysteme lahm legte. Die Auswirkungen dieses Angriffs waren fur viele Menschen auch im Alltag spurbar, weil die Software unter anderem die Ticketautomaten und Anzeigetafeln der Deutschen Bahn abschaltete. Lange Schlangen an den Infocentern vieler Bahnhöfe waren die Folge.

„Der Wirtschaftsstandort Deutschland bleibt ein bevorzugtes Ziel fur Hacker", erklärte BKA-Vizepräsident Peter Henzler. Zudem wurden die Täter immer professioneller. Die Qualität der Angriffe nehme stetig zu. Eine besonders verbreitete Methode ist der Einsatz von sogenannten Bot-Netzen. Täter installieren dabei vom Nutzer unbemerkt automatisiert Schadsoftware auf dessen Computer. Diese ermöglicht den Zugriff auf den PC, von dem beispielsweise sensible Daten wie Kontoinformationen abgeschöpft werden können. Außerdem ist es möglich, die infizierten Computer in ein Netzwerk mit weiteren infizierten Rechnern einzubinden. Diese häufig weltumspannenden Bot-Netze können dann fur massive Angriffe eingesetzt werden, um beispielsweise Webseiten gezielt zu uberlasten. Fur Unternehmen kann das zu hohen Umsatzeinbußen fuhren.

Angriffsziele breit gestreut: Unternehmen, Privatpersonen, Netzwerke

Die Angriffsziele im Bereich Cybercrime reichen dem BKA-Lagebild zufolge von Attacken auf Wirtschaftsunternehmen oder kritische Infrastrukturen, etwa im Energiesektor, bis hin zum Ausspähen privater Handys. Straftaten wurden durch die zunehmende Vernetzung technischer Geräte begunstigt. „Smarte" Kuhlschränke oder Fernseher haben bei der Sicherheit oft Lucken. Zu den Schwachstellen zählen die Sicherheitsbehörden unter anderem voreingestellte Logindaten oder fehlende Sicherheitsupdates. Auch in der Industrie sind Maschinen und Anlagen vernetzt und Steuerungsprozesse webbasiert, weswegen auch hier die Bedrohung durch Cyberkriminalität steigt.

Aufgrund der vermeintlichen Anonymität und der Erreichbarkeit vieler potenzieller Opfer ist das Internet fur Straftäter ein lohnendes Feld, schreibt das BKA in seinem Lagebild. Neben dem offenen Teil des Internets nutzen sie zunehmend das sogenannte Darknet. Dort gibt es Plattformen, auf denen kriminelle Waren wie Waffen oder Rauschgift, aber auch Schadsoftware angeboten werden. Käufer können dort sogar einen Datendiebstahl in Auftrag geben. Diese kriminellen Dienstleistungen werden als „Cybercrime as a Service" bezeichnet und ermöglichen auch technisch wenig versierten Tätern die Begehung von Computerstraftaten.

Die Aufklärungsquote bei Fällen von Computerbetrug lag 2017 bei 40,3 Prozent und stieg damit leicht an. Wichtig sei aber auch die Prävention. Insbesondere bei Geräten des Internets der Dinge sollten schon bei der Herstellung Sicherheitsaspekte noch stärker berucksichtigt werden, forderte das BKA. Gleiches gelte fur mobile Endgeräte.

Donnerstag, 13.09.2018

Milliarden-Schaden für Firmen

Cyberangriffe werden zur alltäglichen Gefahr

Für Industrieunternehmen in Deutschland wird der Schutz vor Hacker-Angriffen immer wichtiger. Allein in den vergangenen zwei Jahren verursachen Cyberattacken auf Industrieunternehmen einen Schaden von mehr als 43 Milliarden Euro.

Sabotage, Datendiebstahl oder Spionage – für Industrieunternehmen in Deutschland sind diese Bedrohungen laut einer Studie des Digitalverbands Bitkom alltägliche Realität. Demnach haben 68 Prozent der Unternehmen innerhalb der vergangenen zwei Jahre einen entsprechenden digitalen Angriff registriert, bei fast der Hälfte der Unternehmen wurde dabei ein Schaden verursacht.

Der Verband errechnete einen Gesamtschaden in Höhe von insgesamt mehr als 43 Milliarden Euro fur diesen Zeitraum. „Mit ihren Weltmarktführern ist die deutsche Industrie besonders interessant für Kriminelle“, sagte Bitkom-Präsident Achim Berg. Befragt wurden für die repräsentativen Ergebnisse 503 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Industriebranchen. Demnach berichtet knapp jedes fünfte Industrieunternehmen, in den vergangenen zwei Jahren Opfer von digitaler Sabotage geworden zu sein, bei elf Prozent wurden etwa E-Mails oder Messenger-Dienste ausgespäht.

Auch klassische analoge Angriffe sind demnach Thema in den Unternehmen, fielen aber vergleichsweise weniger ins Gewicht. So hätten 21 Prozent der Befragten etwa einen Diebstahl sensibler physischer Dokumente, Muster oder Maschinen registriert. „Illegaler Wissens- und Technologietransfer, Social Engineering und auch Wirtschaftssabotage sind keine seltenen Einzelfälle, sondern ein Massenphänomen“, sagte Thomas Haldenwang, Vizepräsident des Bundesamts für Verfassungsschutz, der stellvertretend für den Präsidenten der Behörde, Hans-Georg Maaßen, die Veröffentlichung der Ergebnisse in Berlin begleitete.

Bitkom riet eindringlich zu besserer Vorsorge. „Wer nicht in IT-Sicherheit investiert, handelt fahrlässig und gefährdet sein Unternehmen“, sagte Berg.

Samstag, 11.08.2018

„Digitales Gefechtsfeld" – Bund will in Cyberwaffen investieren

Das Internet ist zum Schlachtfeld für Angriffe auf Staaten geworden. Um für den Cyberwar gerüstet zu sein, plant die Bundesregierung laut einem Bericht mehr Investitionen in die Cybersicherheit. Dies soll über eine Agentur erfolgen.

Die Bundesregierung will einem Bericht zufolge eine eigene Agentur für Cyberwaffen gründen, um in diesem Bereich mit staatlicher Förderung auf dem neuesten Stand der Technik zu sein. Das Bundeskabinett werde am kommenden Mittwoch die Gründung einer „Agentur für Innovation in der Cybersicherheit" zur Stärkung der Sicherheit nach außen und im Inneren beschließen, berichtete der „Spiegel".

Laut der Kabinettsvorlage solle die neue Gesellschaft sicherstellen, dass Sicherheitsbehörden und Bundeswehr für die Abwehr von Cyberangriffen die „technologische Innovations-führerschaft" bei Schlüsseltechnologien selbst behalten und Cyberprodukte zur Analyse oder zum virtuellen Gegenschlag nicht erst vom freien Markt einkaufen müssen.

Die Agentur solle damit einen „nachhaltigen Beitrag zur Sicherung der Zukunft Deutschlands leisten", zitiert das Blatt aus der Vorlage von Verteidigungsministerin Ursula von der Leyen von der CDU und Innenminister Horst Seehofer von der CSU.

Mit der Idee orientiert sich Deutschland demnach an ähnlichen staatlichen Cyberagenturen in den USA oder Israel. Diese identifizierten entscheidende neue Cybertechnologien bereits in der Entwicklungsphase, investierten dann meist in die entsprechenden Start-ups oder Firmen und kämen auf diese Weise an hochmoderne Cyberwaffen, noch bevor diese marktverfügbar seien.

Der „Spiegel" zitiert aus einer Analyse der Bundeswehr, derzufolge die staatliche Cyberforschung für Deutschland notwendig sei, um auf dem „digitalen Gefechtsfeld zu bestehen" und einen „essenziellen Beitrag zur gesamtstaatlichen Sicherheitsvorsorge" zu leisten. Das Verteidigungsministerium habe deswegen für 2019 und 2020 je rund 50 Millionen Euro für Forschung und Technik im Cyber-Sektor eingeplant.