BEILAGE ZUM DSD 1 | 2019

BDSW

INFO
WIRTSCHAFTSSCHUTZ

EINE PUBLIKATION DES ARBEITSKREISES WIRTSCHAFTSSCHUTZ DES BDSW

Vervielfachte Gefahr

→ Der junge Mann, der zum Teil äußerst sensible Daten von gut tausend mehr oder minder prominenten Persönlichkeiten stahl und ins Netz stellte, war alles andere als ein „Hacker" wie wir ihn uns vorstellen. Kein Mensch mit Kapuze, finsterem Blick und alternativem Aussehen, sondern ein ganz normal erscheinender Schüler, der eher schüchtern wirkte. Johannes S., so sein leicht anonymisierter Name, hat gezeigt, dass Hacking, der Angriff auf IT-Infrastrukturen und Daten, längst in der Mitte der Gesellschaft angekommen ist und sich somit die Gefahr, Opfer solcher Attacken zu werden, vervielfacht hat. Nicht nur Firmennetzwerke sind bedroht, sondern auch unsere persönlichen Daten und die unserer Kinder und Kindeskinder.

Wie das BKA ermittelte, hat der junge Mann aus Mittelhessen noch nicht einmal besondere IT-Kenntnisse. Die muss man auch nicht unbedingt haben, wenn man ein Hacker werden will. Im Darknet, dem dunklen Internet parallel zum normalen World Wide Web, können sensible Daten gekauft werden. Erbeutet wurden sie von professionellen Hackern, die nicht selten Berührungspunkte zur organisierten Kriminalität haben. Im Darknet ist es sogar möglich, in einer Art Jobbörse gezielte Hackingaufträge zu vergeben. So steht es sogar „Script Kiddies", sprich blutigen Anfängern in der Hackerszene, offen, ohne eigene physische Anstrengung auf ihre Art Erfolge zu erzielen. Sofern sie über das nötige Kleingeld verfügen.

Ein Finsterling, wie man ihn oft in Filmen sieht. So stellen wir uns Hacker vor. Doch Johannes S., der jüngst durch die Schlagzeilen ging, ist ein eher schüchterner Arztsohn, der noch im Hotel Mama wohnt. Hacking ist längst in der Mitte der Gesellschaft angekommen. Foto: glawo / pixelio.de

Der Fall Johannes S. wirft ein Schlaglicht auf das Themenfeld Hacking. Dennoch ist der junge Mann aus Mittelhessen nur die Spitze des Eisbergs. Die Mehrzahl der Hackingfälle schafft es erst gar nicht in die Schlagzeilen oder in die Nachrichtensendungen. Die Geschädigten legen in den wenigsten Fällen Wert darauf, die Angriffe öffentlich zu machen – und das ist sogar zu verstehen. Wer möchte schon offenbaren, dass es in seinem System Schwachstellen gibt.

Doch Hacking ist allgegenwärtig. Jeder kann zum Opfer werden. Hacker trachten nicht nur nach Firmengeheimnissen, sie lieben auch persönliche Daten und ganz besonders Kontodaten. Das Argument „Warum soll ein Hacker gerade mich angreifen" zieht nicht. Denn einen Menschen ohne „lohnende Ziele", also persönliche Daten, gibt es nicht.

Weil das so ist, möchten wir heute einige Tipps geben, wie man auch in der grundsätzlich unsicheren Umgebung des Internets, ein Stück Sicherheit auf sein Konto verbuchen kann. Hundertprozentige Sicherheit gibt es gerade auch im weltweiten Netz nicht, aber es ist immer möglich, besonders gravierende Lücken zu stopfen und den Grad der Angreifbarkeit zu verringern.

Auch für das Internet gilt: Hacker, besonders solche von der nicht ganz professionellen Sorte, scheuen übermäßigen Aufwand, um an Daten zu kommen. Machen wir ihnen also das Leben schwer.

In diesem Sinne. Bleiben Sie auf der sicheren Seite.

Holger Köster
Vorsitzender
BDSW-Arbeitskreis Wirtschaftsschutz ←

Hacking – ein Massenphänomen, das jeden von uns gleichermaßen betrifft

Von Klaus Henning Glitza

→ Es waren Stars, Politiker und Journalisten, deren Adressen, Mailings und Dokumente gehackt und in der Vorweihnachtszeit veröffentlicht worden waren. Der Promi-Faktor, der dieses Thema beflügelt hat, darf jedoch nicht darüber hinwegtäuschen, dass Hacking ein Massenphänomen ist, das jeden von uns gleichermaßen betrifft.

Die Gefahr ist alltäglich. Im Sekundentakt werden viele kleine und mittelständische Unternehmen, aber auch Home-Office-Arbeiter und Privatleute angegriffen. Sie haben zumeist keine IT-Abteilung oder Sicherheitsexperten im Rücken und sind deshalb, mehr noch als Promis, Hackers Liebling.

Wohin führt das? Es ist keinesfalls eine Übertreibung, das Internet als Haifischbecken zu bezeichnen. Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) waren es im vergangenen Jahr sage und schreibe 800 Millionen Schadprogramme, die im Umlauf waren, eine gewaltige Zahl, die jeden Tag nach oben korrigiert werden muss. Denn alle 24 Stunden kommen 390.000 neue Varianten hinzu. Doch trotz dieser schwindelerregenden Zahlen herrscht hierzulande eine „erstaunliche digitale Sorglosigkeit", wie es erst jüngst Nordrhein-Westfalens Innenminister Herbert Reul beklagte.

„Angriffe auf die Informationsinfrastrukturen im Cyber-Raum werden zunehmend komplexer und professioneller", konstatiert das BSI. Die Promi-Attacke nimmt sich fast schon harmlos gegen die Aktivitäten fremdstaatlich gelenkter Hacker gegen kritische Infrastrukturen und staatliche sowie politische Institutionen aus. Die USA, die Volksrepublik China und die Russische Föderation liefern sich regelrechte Hackerschlachten. Trotzdem nimmt die IT-Abhängigkeit von Unternehmen, Staat und Bürgern ständig zu.

Ein schwaches Passwort zu knacken? Für gewiefte Hacker ist das eine Fingerübung. Ein starkes Passwort ist deshalb ein immens wichtiger Zugangsschutz, der ungebetene Besucher fernhalten kann. Foto: Bernd Kasper / pixelio.de

Dabei ist es möglich, bereits mit ein paar Schritten zumindest für einen Basisschutz sorgen. Vorausgeschickt sei, dass niemand besser für seine Sicherheit sorgen kann als wir selbst. Nach dem Staat zu rufen ist ein populär erscheinender Schritt. Aber wollen wir das überhaupt, dass sich der Staat um alles kümmert? Wir müssen uns erst einmal an die eigene Nase fassen. Tun wir selbst alles, um unsere Sphären zu schützen? Der Staat kann nicht alles richten und jede sperrangelweit geöffnete Haustür bewachen. Für unsere eigene IT-Sicherheit müssen wir selbst sorgen. Erst wenn alles Menschenmögliche getan ist, können wir berechtigterweise nach „Vater Staat" rufen.

Faktum ist, es gibt in vielen Bereichen Sicherheitsdefizite. Das fängt mit den Zugangsdaten an. Passwörter zu knacken, ist kein großes Thema für gewiefte Hacker. Kaum zu glauben, aber wahr: Aus Angst, das Passwort zu vergessen, wählen viele Anwender einfachste Passwörter. Nach Angaben des BSI stehen phantasielose Passwörter wie „123456" oder „qwert" auf der Hitliste ganz oben. Ebenso problematisch ist es, wenn ein einziges Passwort für alles verwendet wird. Für viele Internetdienste, selbst für Newsletter, müssen sich die Nutzer anmelden und häufig ein Passwort vergeben. Es soll den Internetdiensten nichts Negatives unterstellt werden, aber Hand aufs Herz, was wissen wir wirklich über diese Anbieter? Welche Infos haben wir über deren IT-Sicherheit und die von deren Mitarbeitern? Selbst wenn beim Internetdienst höchste Sicherheit garantiert ist, können wir ausschließen, dass der Internetdienst nicht längst gehackt ist? Fast täglich erreichen uns Nachrichten, dass Dienste und Datenbanken angegriffen worden sind und dabei Millionen von Daten „verloren" gingen.

Genauso fatal ist es, ein Passwort zu wählen, das in einem Wörterbuch stehen könnte. In Filmen sind oft Hacker zu sehen, die händisch alle möglichen Zeichenfolgen ausprobieren. Alles Schnee von gestern. Die Hacker verfügen schon seit längerem über Tools, die komplette Lexikainhalte samt Zahlenkombinationen durchtesten, bis der Zugang gelingt.

Abwehrmaßnahme: Für jeden Zugang ein eigenes Passwort. Jede Wiederholung ist ein immenses Sicherheitsrisiko. Gute Passwörter sollten möglichst lang sein sowie Groß- und Kleinschreibung und Sonderzeichen enthalten. Und möglichst „unsinnig" sein, sprich sich in dieser Form in keinem Wörterbuch

Das Internet bietet nahezu unbegrenzte Möglichkeiten. Kehrseite ist, dass sich die Benutzer auch die Risiken und die geballte kriminelle Energie einer aus den Fugen geratenen Welt ins Haus holen.
Foto: Thorben Wengert / pixelio.de

wiederfinden. Beispiel: Nicht Frankfurt, sondern Furtefrankonia. Und: Das gute alte Notizbuch ist besser als der teuerste Daten- oder Kennwortspeicher. Auf das Notizbuch hat der professionellste Hacker keinen Zugriff. Natürlich darf diese Erinnerungshilfe nicht offen herumliegen.

Halten Sie Ihr Betriebssystem auf dem Laufenden. Von Windows und Co. werden regelmäßig Updates angeboten. Machen Sie davon unbedingt Gebrauch bzw. schalten Sie die automatische Updatefunktion frei. Updates haben eine große Bedeutung. Sie sind das A und O für Ihre Internetsicherheit.

Dazu ein kleiner Exkurs. Unter dem wachsenden Konkurrenzdruck werden Betriebssysteme oft mit heißer Nadel entwickelt. Marketing geht vor Präzision. Vereinfacht ausgedrückt könnte man sagen, es kommt ein nur ungenügend getestetes Produkt in den Handel, das dann nach und nach durch Updates komplettiert wird. Diese auch Patches genannten „Nachrüstungen" dienen vor allem der Sicherheit. Denn die in Eile programmierten Betriebsprogramme weisen oft Fehler auf, die von Angreifern genutzt werden können. Mit jedem Update werden diese Falschprogrammierungen eliminiert.

Verlassen Sie sich nicht allzu sehr auf Virenscanner. Auch das beste dieser Programme kann nur ein Basic der IT-Sicherheit sein – nicht mehr und nicht weniger. Anti-Viren-Scanner können nur bekannte und öfter auftretende Schadprogramme detektieren. Eigens für einen spezifischen Angriff geschriebene Trojaner fallen durch das Rost.

Aktualisieren Sie das Anti-Viren-Programm täglich und lassen Sie alle 24 Stunden den Scanner einmal durchlaufen. Bevorzugen Sie bekannte Programme, die Ihre Datenbank mehrmals täglich aktualisieren.

Angriffe können auch aus einer unerwarteten Richtung kommen. So wurden Telefaxgeräte in einigen Fällen von professionellen Hackern als Einfallstor in Firmennetzwerke genutzt. Auch Drucker haben vielfach eine Faxfunktion, die angreifbar ist – egal ob sie genutzt wird oder nicht. Das funktioniert natürlich nur dann, wenn die Faxgeräte/Drucker ungesichert mit dem Firmennetzwerk verbunden sind. Der Sicherheitsexperte Yaniv Balmas warnt, dass Faxgeräte eine „antike Technologie" von vorgestern seien, „deren Protokolle sich in 30 Jahren nicht geändert haben". Besonders heimtückisch: Hacker, die Kontrolle über das Gerät erlangt haben, können sich gestohlene Dokumente selbst als Fax schicken. Wer sein Netzwerk sicherheitstechnisch auf dem neusten Stand hält, tut trotzdem zu wenig, wenn er Faxgeräte/Drucker mit Faxfunktion komplett in sein Netzwerk integriert. Maßstab ist das schwächste Glied in der Kette – und Hacker wären keine Hacker, wenn sie das nicht wüssten.

Schutzmaßnahme: Kein Netzwerk für alles, sondern ein separates Netzwerk nur für Faxgeräte und Drucker.

Allgemeine Hinweise: Keine Anhänge in Mails öffnen, deren Absender Sie nicht kennen. Sie könnten Schadsoftware enthalten, die Hackern den Zugang zu Ihrem System ermöglicht oder den PC beschädigt. Besonders kritisch ist es, wenn Sie aufgefordert werden, einen Anhang zu öffnen oder einen Link anzuklicken. Ein untrügliches Anzeichen für eine Fake-Mail ist es, wenn Sie nicht mit Ihrem Namen angeschrieben werden. Oft enthalten trojanische Mails auch keine detaillierten Absenderangaben. Möglich ist es aber auch, dass unter „falscher Flagge" gesegelt wird. So unter dem Namen eines Anbieters, den nahezu alle kennen: Geldinstitute, Kreditkartenunter-

Ein sicheres Passwort darf sich in keinem Wörterbuch wiederfinden. Bilden Sie „unsinnige" Kombinationen. Oder nutzen Sie die Eselsbrücke, indem Sie einen Satz bilden, den Sie sich gut merken können, und dann nur die Anfangsbuchstaben verwenden. Beispiel: Meine getigerte Katze Lilly ist ein gutes Tier, das viel und oft schnurrt = MgKLiegT,dvuos. Optimal wäre noch ein Sonderzeichen dazu.
Foto: Bernd Kasper / pixelio.de

nehmen, Stadtwerke, Mailprovider. Doch auch in solchen Fällen fehlt in der Regel die korrekte Anrede.

Auch beliebt: Angebliche Avancen von Damen und Herren, die Sie wiedersehen möchten. Gerne werden auch aktuelle Ereignisse genutzt, zum Beispiel Umweltkatastrophen, um Sie zum Öffnen eines Anhangs oder eines Links zu verleiten. Fragen Sie sich in solchen Fällen immer: Welchen Anlass sollte eine seriöse Institution haben, Sie per Mai zu kontaktieren? Normalerweise wird der Postweg oder ein Telefonat gewählt.

Und: Seien Sie vorsichtig mit Datenträgern (CD-ROM, Sticks), die Ihnen ohne erkennbaren Bezug zugeschickt werden. Wenn Sie diese Speichermedien trotzdem öffnen möchten, benutzen Sie einen PC, der nicht mit einem Netzwerk verbunden ist.

Es gibt viele weitere Schritte, Ihr Netzwerk sicherer zu machen. Zum Beispiel Tools, die verdächtige Prozesse detektieren, externe Festplatten, auf denen Sie – für Angreifer unerreichbar – verschlüsselt Ihre sensiblen Dateien ablegen können, Abkopplungen vom allgemeinen Netzwerk. Lassen Sie sich von einem vertrauenswürdigen IT-Sicherheitsexperten beraten. Dessen Kosten bilden einen Bruchteil von dem, was Sie bei einem geglückten Hackerangriff aufwenden müssten. ←

Die im Dunkeln sieht man nicht... Ein Job für Feiglinge: Hacker können aus der Anonymität heraus agieren und ihre Angriffe irgendwo auf der Welt starten. Foto: Bernd Kasper / pixelio.de

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Dr. Berthold Stoppelkamp
Leiter des Hauptstadtbüros des BDSW und zuständiges Geschäftsführungsmitglied für den Arbeitskreis Wirtschaftsschutz

Bitkom-Umfrage: Cyberkriminalität

→ Als Ergebnis einer repräsentativen Umfrage unter mehr als tausend Internetnutzern in Deutschland stellte sich heraus, dass jeder zweite Nutzer (50 Prozent) in 2018 Opfer von Cyberkriminalität (Datendiebstahl, Identitätsklau, Beleidigung oder Betrug) geworden ist. Jeder vierte Nutzer (23 Prozent) war von der illegalen Verwendung persönlicher Daten betroffen. Vom Missbrauch seiner Kontodaten war jeder Neunte Internetnutzer (11 Prozent) betroffen. **www.bitkom.org** ←

BSI-Empfehlungen zum Schutz vor Datendiebstahl

→ Das BSI gibt Tipps, wie der Internetnutzer mehr Datensicherheit erreichen kann und sich somit besser gegen Cyberkriminelle wappnen kann. Insbesondere sollte dort, wo es technisch möglich ist, eine Zwei-Faktor-Authentisierung genutzt werden.
www.bsi.bund.de ←

„Stiftung Datenschutz"-Broschüre: Datenschutz im Betrieb

→ Arbeitgeber und Beschäftigte müssen sich mit den Kernpflichten des Datenschutzes auskennen. Die Broschüre wurde an die Anforderungen der EU-Datenschutz-Grundverordnung aus dem Mai 2018 angepasst und vermittelt kompakt und praxisnah die notwendigen Anforderungen an einen aktuellen betrieblichen Datenschutz. **www.stiftungdatenschutz.org** ←

BSI-Empfehlungen für Betroffene eines Datenleaks

→ In jüngster Vergangenheit ist die Veröffentlichung hunderter überwiegend privater und persönlicher Datensätze von Politikern und Prominenten bekannt geworden. Das BSI gibt Hinweise, was zu tun ist, wenn ein Internetnutzer den begründeten Verdacht hat, dass sich Unbefugte auf eines oder mehrere Online-Konten Zugriff verschafft haben. **www.bsi.bund.de** ←

BDSW

BDSW BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT

Verantwortlich: Dr. Berthold Stoppelkamp
Redaktion: Klaus Henning Glitza

Norsk-Data-Straße 3 · 61352 Bad Homburg
Fon: +49 6172 948050 · Fax: +49 6172 458580

Mail: mail@bdsw.de
Web: www.bdsw.de