Datum: 28.07.2017

DAS SCHWEIZER WIRTSCHAFTSMAGAZIN
BILANZ

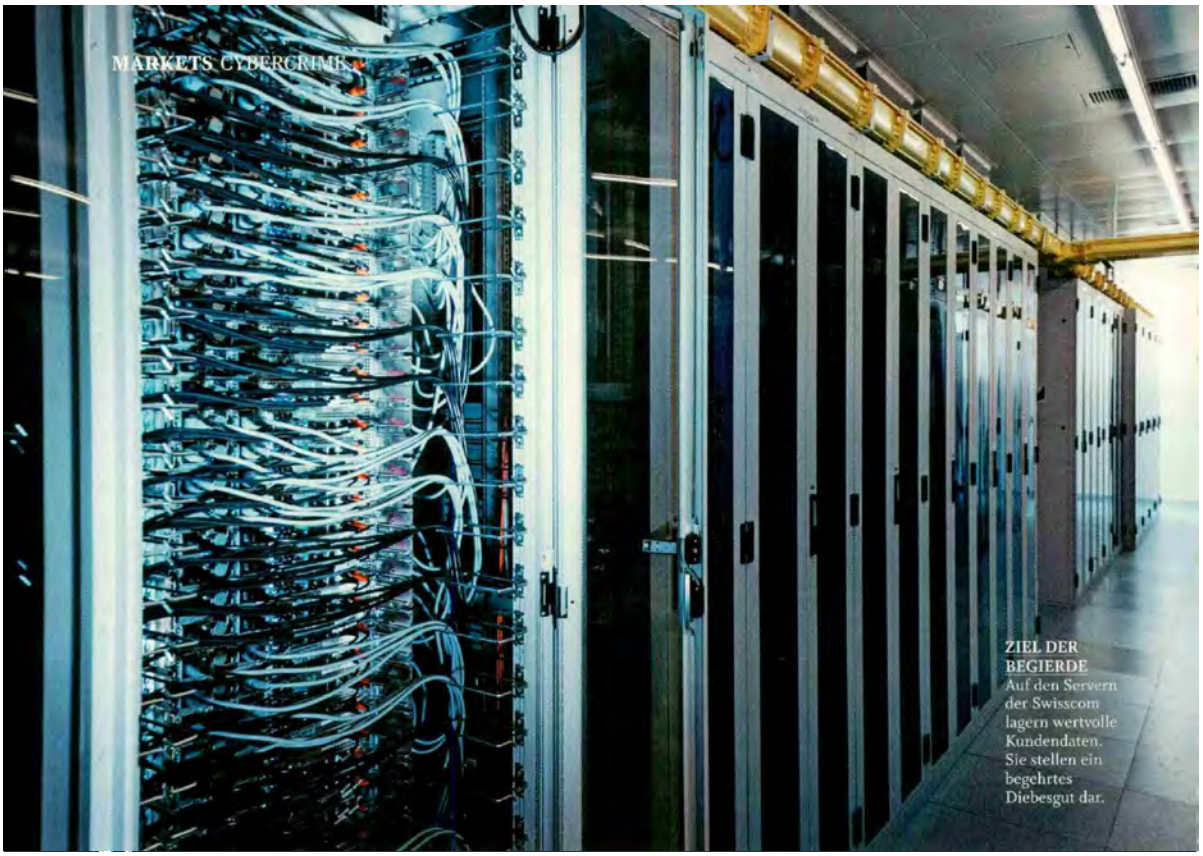
BILANZ
8021 Zürich
058 269 22 00
www.bilanz.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 41'931
Erscheinungsweise: monatlich

Seite: 72
Fläche: 248'947 mm²

Auftrag: 1000033
Themen-Nr.: 999.010

Referenz: 66173465
Ausschnitt Seite: 1/7



ZIEL DER BEGIERDE Auf den Servern der Swisscom lagern wertvolle Kundendaten. Sie stellen ein begehrtes Diebesgut dar.

Verbrechen lohnt sich

Cyber-Attacken Die Zahl der Angriffe auf Schweizer Unternehmen steigt rapide. Industriespionage verlagert sich ins Netz.

von HOLGER ALICH

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG
ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch

Datum: 28.07.2017

DAS SCHWEIZER WIRTSCHAFTSMAGAZIN
BILANZ

BILANZ
8021 Zürich
058 269 22 00
www.bilanz.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 41'931
Erscheinungsweise: monatlich

Seite: 72
Fläche: 248'947 mm²

Auftrag: 1000033
Themen-Nr.: 999.010

Referenz: 66173465
Ausschnitt Seite: 2/7

SCHNELLE EINGREIFTRUPPE
Bei Swisscom rückt das Team von Lorenz Inglin aus, wenn ein Rechner des Konzerns mit Schadsoftware befallen ist. Sein Incident-Response-Team verfügt über Spezialkoffer, mit deren Hilfe sich Beweise auf gehackten Rechnern sichern lassen.

Lorenz Inglin hatte sich auf einen gemütlichen Abend mit Freunden und der Familie gefreut. Statt Computerbildschirme überwachte der IT-Spezialist der Swisscom Bratwürste, die auf dem Grill brutzelten. Da klingelte sein Handy. Und der Grillabend war vorbei.

Denn am anderen Ende der Leitung war einer von Inglins Sicherheitsspezialisten. Dieser hatte bei der Netzüberwachung etwas Merkwürdiges entdeckt: Ein Laptop eines höheren Swisscom-Kadermitarbeiters baute eine Verbindung zu Netzen im Ausland auf, wo dieser Rechner normalerweise nichts zu suchen hatte. «Also fuhr ich sofort ins Büro», erzählt Inglin, denn der IT-Ingenieur ist Leiter des Incident-Response-Teams der Swisscom. Sprich: Er leitet die schnelle Eingreiftruppe gegen Hacker. Inglin liess den fraglichen Rechner noch am selben Abend sperren und am nächsten Tag sicherstellen und untersuchen. Und tatsächlich: Über eine spezielle Malware sollten vom Rechner des Kadermanns, der in der Produktentwicklung der Swisscom arbeitet, offenbar Geschäftsgeheimnisse gestohlen werden. «Die Malware war gut gemacht und ein Unikat, der Angriff war sehr professionell», erinnert sich Inglin an den Vorfall aus dem Jahr 2015. Die Schadsoftware war dem Mitarbeiter über eine persönlich an ihn gerichtete Mail untergejubelt worden.

Ausdrücke wie Hacking, Phishing oder Ransomware (siehe Glossar auf Seite 73) waren früher nur eingefleischten Nerds ein Begriff. Heute muss sich jeder Chef eines KMU damit beschäftigen. Das Internet zeigt immer stärker seine dunkle Seite. «Die

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG
ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch

Datum: 28.07.2017

DAS SCHWEIZER WIRTSCHAFTSMAGAZIN
BILANZ

BILANZ
8021 Zürich
058 269 22 00
www.bilanz.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 41'931
Erscheinungsweise: monatlich

Seite: 72
Fläche: 248'947 mm²

Auftrag: 1000033
Themen-Nr.: 999.010

Referenz: 66173465
Ausschnitt Seite: 3/7

Qualität der Angriffe hat stark zugenommen, die Mails, in der Schadsoftware versteckt wird, sind kaum mehr von authentischen Schreiben eines Dienstleisters oder Kunden zu unterscheiden», sagt Christian Funk, Leiter des deutschen Forschungs- und Analyseteams bei Kaspersky Lab. «Wir haben beobachtet, dass die Angreifer vermehrt KMUs ins Visier nehmen», warnt Pascal Lamia, Chef der Melde- und Analysestelle Informationssicherung (Melani).

200 000 FIRMEN BETROFFEN

In den vergangenen Monaten haben Attacken mit sogenannter Ransomware wie WannaCry oder NotPetya für Schlagzeilen gesorgt. Die Schadprogramme sperren die Computer der Nutzer, die Angreifer wollen die Daten erst gegen Lösegeldzahlungen freigeben. Die Schweiz kam bisher glimpflich davon, wohl auch, weil Unternehmen ihre Software meist auf dem neuesten Stand halten. Laut der Meldestelle Melani waren hierzulande rund 200 Firmen betroffen - weltweit waren es über 200 000. In Grossbritannien gingen zum Beispiel reihenweise Krankenhäuser wegen WannaCry in die Knie.

Beim ausgefeilteren Angriff mit NotPetya, der wenige Wochen später er- ▸

▸ folgte, waren in der Schweiz wahrscheinlich acht Firmen betroffen. Am 26. Juni gegen 14 Uhr wurden beim Werbevermarkter Admeira, der auch für BILANZ die Anzeigenplätze verkauft, auf einmal alle Monitore schwarz. Als die Mitarbeiter die Rechner wieder hochfuhren, sahen sie die Erpresseraufforderung, Bitcoin im Wert von 300 Dollar zu zahlen. «Rund 200 von 300 Rechnern waren betroffen, das Schadprogramm kam aber nicht per Mail, sondern vermutlich über ein vernetztes Laufwerk», berichtet Marc Sier, COO von Admeira. Via Twitter und Telefon informierte das Unternehmen sofort die Kunden über die Probleme. Fast eine Woche dauerte es, bis alles wieder normal lief. «Der Schaden hält sich in Grenzen, denn Umsatz haben wir so gut wie keinen verloren, das Kerngeschäft konnte zu jeder Zeit sichergestellt werden», so Sier.

UNBEKANNTES AUSMASS

Über das gesamte Ausmass an Cyberattacken wie jener auf Admeira gibt es für die Schweiz keine validen Daten. Denn eine allgemeine Meldepflicht gibt es nicht, wird aber derzeit diskutiert. Eine Ahnung von der Grösse des Phänomens geben die Verdachtsmeldungen, die Nutzer beim Bundesamt für Polizei (Fedpol) einreichen (siehe Grafik auf Seite 73).

In nur zwei Jahren ist die Zahl der Meldungen um fast 40 Prozent auf rund 14 000 gestiegen. Die Zahl der eingereichten Strafanzeigen ist dagegen um einiges geringer: Laut dem Bundesamt für Statistik waren es letztes Jahr knapp 4800. Längst nicht alle Opfer schalten die Behörden ein. «Die Dunkelziffer ist enorm», sagt daher Stephan Walder. Der Staatsanwalt ist Co-Leiter des Kompetenzzentrums Cybercrime des Kantons Zürich. Auch zum Schadenvolumen gibt es keine verlässlichen Daten. Lloyd's of London taxiert dieses Volumen bei Firmen weltweit auf 400 Milliarden Dollar - pro Jahr, wohlgemerkt.

Doch wer sind die Täter? Swisscom-Experte Inglin hat fünf Gruppen identifiziert. «Die gefährlichsten sind staatlich

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG
ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch

Datum: 28.07.2017

DAS SCHWEIZER WIRTSCHAFTSMAGAZIN
BILANZ

swisscom

BILANZ
8021 Zürich
058 269 22 00
www.bilanz.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 41'931
Erscheinungsweise: monatlich

Seite: 72
Fläche: 248'947 mm²

Auftrag: 1000033
Themen-Nr.: 999.010

Referenz: 66173465
Ausschnitt Seite: 4/7

unterstützte Angreifer, die oft Wirtschaftsspionage betreiben», erklärt er. Nordkorea sei hier in letzter Zeit verstärkt aktiv geworden, China und Russland sowie die USA seien Ursprungsländer. «Staatliche Hackergruppen, konkret auch aus China, nehmen die Schweiz verstärkt ins Visier», warnt auch Reto Häni. Er ist Partner und Leiter Cybersecurity bei der Unternehmensberatung PwC Schweiz. Er sieht gar einen Zusammenhang zwischen Chinas Plänen zum Aufbau strategischer Sektoren und der beobachteten Hackingaktivität.

Als zweitgefährlichste Gruppe sieht Inglin Cyberterroristen. Die dritte umfasst kriminelle Angreifer, denen es primär um Geld geht. «Dann gibt es politische Aktivisten», sagt Inglin. Bekanntestes Beispiel hierfür ist Anonymous. Die fünfte Gruppe in Inglins Bedrohungspyramide bilden die sogenanten «Script Kiddies», zumeist jugendliche Tüftler, die ohne jegliches Unrechtsbewusstsein versuchen, in Systeme einzudringen.

Wie raffiniert zuweilen Cyberbetrüger vorgehen, zeigt das Beispiel zweier 30-jähriger Rumänen, die im April zu mehrjährigen Haftstrafen verurteilt wurden, nachdem sie vom Zürcher Cybercrime-Team dingfest gemacht worden waren. Die Täter hatten fingierte Wohnungsanzeigen auf Immobilienportale geschmuggelt. Da in Zürich Wohnungen knapp sind, hatten Interessenten ohne Besichtigungstermin eingewilligt, vorab ein Depot von 2365 Franken zu überweisen. Es gab 2249 Interessenten für die fiktiven Wohnungen, elf haben laut Urteil am Ende tatsächlich gezahlt.

Der Einstieg in die Cyberkriminalität ist denkbar einfach: Auf Marktplätzen im Darknet wie AlphaBay gibt es Erpressungssoftware schon zur Miete. Beim Anbieter «RaasBerry» kostet beispielsweise das Bronze-Paket nur 60 Dollar im Monat. «Sie bekommen 100 Prozent der von den Opfern erpressten Gelder», heisst es im Angebot. Im «Command and Control»-Center kann der Auftraggeber prüfen, wie viele Rechner schon infiziert sind.

Für den Wirtschaftsstandort Schweiz gefährlicher sind dagegen Spionageattacken, wie sie die Swisscom schon erlebt hat. Dabei dauert es durchschnittlich 270 Tage, bis ein Netzeindringling entdeckt wird. Das ist das Ziel der Angreifer: Je länger sie sich unbemerkt im Netz des Opfers bewegen können, desto mehr Administratorpasswörter können sie sich aneignen und immer weiter vordringen. Nach diesem Muster gingen die Täter beim Angriff auf die Ruag vor. Über ein Jahr lang hatten sie sich auf den Rechnern des Rüstungskonzerns getummelt, bevor sie entdeckt wurden.

Kurz vor Weihnachten 2015 sass Bruno Blumenthal in einer Schulung, als der Sicherheitsexperte der Ruag einen Telefonanruf bekam. «Ein Mitarbeiter der Cybersecurity informierte mich, dass er eine Warnung vom Nachrichtendienst bekommen habe», erinnert er sich. «Dieser wiederum hatte einen Tipp von einem befreundeten Nachrichtendienst erhalten, dass verdächtige Kommunikation von einer unserer IP-Adressen entdeckt worden sei.»

Der Tipp war allerdings recht allgemein gehalten. Zusammen mit Experten der Meldestelle Melani suchten die Ruag-Verantwortlichen nach einem möglichen Datenleck. Zunächst ohne grossen Erfolg. «Richtig los ging es Ende Januar», berichtet Blumenthal. Denn erst dann rückte der Partner-Geheimdienst, von dem der Sicherheitsexperte nicht sagen will, um wen es sich handelt, heraus, an welchen Rechner im Ausland die Informationen der Ruag flossen. «Es war die gehackte Website eines deutschen Dartvereins», so Blumenthal. Sie diente allerdings lediglich als Umschlagplatz, um die gestohlenen Daten weiterzuleiten. Doch mit Hilfe der Info, wohin die Daten flossen, konnten Blumenthal und sein Team feststellen, wo im eigenen Haus das Leck war.

ERFOLGLOSE ERMITTLER

Insgesamt seien «weniger als zehn» Rechner mit Schadsoftware infiziert worden. Und keiner davon habe Zugang zu als «vertraulich» oder «geheim» klassifizierten Informationen von Kunden oder schützenswerten Technologien gehabt, versichert Blumenthal. Da aber die Verbindungsdaten nicht länger als zwölf Monate gespeichert werden, konnten die Experten nicht mehr exakt feststellen, wann genau der erste Angriff stattgefunden hatte. Vermutlich war es Ende 2014. Auch die Identität des Angreifers ist bis heute unklar. Ermittlungen der Schweizer Bundesanwaltschaft haben bisher kein Ergebnis gezeitigt.

Bekannt ist nur, dass sich die Hacker russischer Technik bedienten, genauer gesagt Schadprogrammen der Turla-Familie. «Das muss aber nicht zwingend heissen, dass der Angreifer auch aus Russland stammt», so Blumenthal. Insgesamt umfasste der abgezogene Datenverkehr 20 Gigabyte. «Den genauen Inhalt kennen wir nicht, der Angreifer interessierte sich offenbar für unsere Projekte mit dem Verteidigungsdepartement», so Blumenthal. Da aber die befallenen Rechner keinen Zugang zu Geheiminformationen hatten, schliesst die Ruag aus, dass sensible Daten gestohlen wurden.

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG
ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch

Datum: 28.07.2017

DAS SCHWEIZER WIRTSCHAFTSMAGAZIN
BILANZ

BILANZ
8021 Zürich
058 269 22 00
www.bilanz.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 41'931
Erscheinungsweise: monatlich

Seite: 72
Fläche: 248'947 mm²

Auftrag: 1000033
Themen-Nr.: 999.010

Referenz: 66173465
Ausschnitt Seite: 5/7

Die Ruag betont, dass sie Konsequenzen gezogen habe. So wurde ein zweistelliger Millionenbetrag in die Verbesserung der IT-Sicherheit investiert. «Zudem haben wir Anfang 2016 für Mitarbeitende und Kunden eine topmodern ausgestattete Cyber Training Range errichtet», sagt Blumenthal. Hier können Attacken simuliert werden, um IT-Spezialisten zu trainieren.

«Die Attacke auf die Ruag war neben dem Angriff auf das Netz ▸

▸ des Eidgenössischen Departements für auswärtige Angelegenheiten aus dem Jahr 2009 der bisher schwerste Fall im Bereich der Cyberspionage in der Schweiz», sagt Pascal Lamia von Melani. Zumindest sind es jene Fälle, über die er sprechen kann. Denn aus Sorge um ihre Reputation sind Unternehmen erpicht darauf, dass erfolgreiche Hackerattacken möglichst nicht öffentlich werden. Dabei laufen just in diesem Moment international koordinierte und erfolgreiche Hackerangriffe, bei denen es auch Opfer in der Schweiz gibt.

ANGRIFFIGER PANDA

Die Rede ist vom Hackernetzwerk APT10, dessen Herkunft in China vermutet wird und das auch unter dem Namen «Stoned Panda» bekannt ist. Laut einem Report von PwC und BAE Systems sei es dieser Gruppe gelungen, die Rechner von IT-Dienstleistern anzugreifen. Die Hacker nutzen aus, dass immer mehr Unternehmen ihre IT an Drittunternehmen auslagern, um Kosten zu senken. Die Systeme der Serviceprovider sind zwar sehr gut geschützt, doch der Aufwand für staatliche Hacker lohnt sich: Sind sie einmal drin, haben sie Zugang zu Daten von Hunderten Kunden. Opfer gibt es laut dem Bericht unter anderem in Japan, den USA, Kanada, Frankreich, Grossbritannien - und eben der Schweiz.

PwC Schweiz sind nach eigenen Angaben hierzulande mehrere Opfer bekannt, die durch die sogenannte «Operation Cloud Hopper» vermutlich Daten verloren haben: ein Industrie- und ein Serviceunternehmen. Namen nennt PwC Schweiz keine, auch nicht von den gehackten IT-Dienstleistern. Es handle sich jedoch nicht um Kunden aus dem Finanzsektor, die oft als primäres Ziel von solchen Angriffen wahrgenommen würden, heisst es. Auch Pascal Lamia wird einsilbig, wenn man ihn auf die Gruppe ATP10 anspricht: «Wir haben Erkenntnisse zu APT10, äussern uns aber nicht dazu, um laufende Abklärungen nicht zu stören.»

Es ist schwierig, Hacker im Netz zu entdecken - noch schwerer allerdings ist es, sie dingfest zu machen. Davon weiss Stephan Walder zu berichten, Staatsanwalt und Co-Leiter des Kompetenzzentrums Cybercrime des Kantons Zürich. Zwölf Experten der Staatsanwaltschaft sowie von Kantons- und Stadtpolizei jagen in diesem landesweit bisher einmaligen Zentrum Verbrecher aus dem Cyberspace. «Die Probleme fangen schon damit an, dass es nicht in allen Ländern die gesetzliche Pflicht zur Vorratsdatenspeicherung gibt», sagt Walder. In der Schweiz löschen die Fernmeldedienstanbieter die Verbindungsdaten nach sechs Monaten.

Erschwerend kommt hinzu, dass die Täter in den meisten Fällen aus mehreren Ländern heraus aktiv sind - und Stephan Walders Team so auf langwierige Verfahren angewiesen ist. Die meisten Rechtshilfebegehren gehen in die USA, denn dort sitzen die grossen Social-Media-Konzerne. Zwischen drei und achtzehn Monate kann es dauern, bis die US-Justiz auf Gesuche antwortet. Die Angaben aus den USA führen dann etwa zu Internetadressen von Verdächtigen in anderen Ländern - sodass Walder und sein Team jeweils neue Rechtshilfeanträge stellen müssen.

Im vergangenen Jahr hat sein Team 109 Fälle abgeschlossen, doch nur in 35 Prozent erfolgte eine Anklage oder ein Strafbefehl. Wie im Fall der Cyberbetrüger mit ihren fingierten Wohnungsanzeigen. In Bosnien konnten die lokalen Behörden in einem internationalen Grossverfahren mit Beteiligung des Kompetenzzentrums Cybercrime Hacker verhaften, die Schweizer Banken mit der Drohung erpresst hatten, deren Server mit einer DDoS-Attacke lahmzulegen.

GRUSS VON FRED777

Die Swisscom übergibt einen oder zwei Fälle pro Jahr an die Staatsanwaltschaft. Der Netzbetreiber setzt verstärkt auf Prävention. Ein eigenes Team durchsucht dafür das Darknet. So etwa Dirk Peters (Name geändert), der Foren wie «Back2hack» durchforstet. In bestimmte Diskussionsgruppen gelangen Teilnehmer nur auf Einladung. Peters sitzt vor seinem Laptop in einem Büro mit zugezogenen Vorhängen. Auch die Kollegen sollen nicht sehen, woran er arbeitet.

«Wir beteiligen uns unter falscher Identität an Diskussionen und werden per Mail über neue Einträge informiert», erklärt Peters, «auf diese Weise bekommen wir mit, was potenziell gefährliche Akteure so machen.» Er zeigt auf einen Eintrag

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG
ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch

Datum: 28.07.2017

DAS SCHWEIZER WIRTSCHAFTSMAGAZIN
BILANZ

BILANZ
8021 Zürich
058 269 22 00
www.bilanz.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 41'931
Erscheinungsweise: monatlich

Seite: 72
Fläche: 248'947 mm²

Auftrag: 1000033
Themen-Nr.: 999.010

Referenz: 66173465
Ausschnitt Seite: 6/7

des Forumteilnehmers «fred777». «Habe Sicherheitslücke bei einer Rüstungsfirma gefunden», rühmt sich dieser und erbittet Hilfe, um diese Lücke auszunutzen.

Swisscom will nun ihre Bedrohungsanalysen zu einem Geschäftsfeld ausbauen. «Was wir für das eigene Haus tun, wollen wir unseren Grosskunden anbieten», sagt Lorenz Inglin. «Dafür möchten wir neue Experten einstellen.» Swisscom will damit aus der Not eine Tugend machen: mit Cyberabwehr auch noch Geld verdienen. ■

Firmen schalten selten die Staatsanwaltschaft ein. Sie haben Angst, dass eine Attacke publik wird.

Die Experten von Lloyd's of London taxieren das Schadenvolumen bei Unternehmen auf 400 Milliarden Dollar im Jahr.

SCHWIERIGE SPURENSUCHE
Im Schnitt dauert es 270 Tage, bis Hacker in Systemen entdeckt werden. Oft sind Verbindungsdaten dann gelöscht. Das erschwerte auch die Arbeit von Bruno Blumenthal, der als IT-Sicherheitsexperte den Hackerangriff beim Staatskonzern Ruag aufarbeitete.

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG
ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch

Datum: 28.07.2017

DAS SCHWEIZER WIRTSCHAFTSMAGAZIN
BILANZ

BILANZ
8021 Zürich
058 269 22 00
www.bilanz.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 41'931
Erscheinungsweise: monatlich

Seite: 72
Fläche: 248'947 mm²

Auftrag: 1000033
Themen-Nr.: 999.010

Referenz: 66173465
Ausschnitt Seite: 7/7

Kleines Abc der Hacker

DDoS-Angriff: **Attacke, um die Server eines Opfers lahmzulegen. Hacker übernehmen die Kontrolle von schlecht geschützten Rechnern oder Geräten, die mit dem Netz verbunden sind, wie zum Beispiel TV-Geräte, und lassen diese dann die gleiche Website aufrufen, etwa von einem Online-Shop. Die Server des Opfers sollen unter der Last der Anfragen zusammenbrechen, wie geschehen bei Digitec und Galaxus im vergangenen Jahr.**

Phising: **Versuche, an Zugangsdaten heranzukommen, zum Beispiel für das E-Banking. Dabei wird dem Opfer eine gefälschte Mail seiner Bank oder seines Telekomanbieters geschickt, in welcher der Nutzer aufgefordert wird, auf einen Link zu klicken, um seine Daten zu aktualisieren. Der Link führt jedoch auf eine gefälschte Website, wo die Zugangsdaten abgegriffen werden sollen.**

Ransomware: **Oberbegriff für Schadprogramme wie WannaCry oder NotPetya, die den Bildschirm oder die Festplatte eines befallenen Computers sperren und erst gegen Zahlung eines Lösegeldes wieder freigeben. Die Bezahlung erfolgt in der Regel in Bitcoin. Die Zahlung garantiert indes nicht die Freigabe, daher empfehlen Experten, niemals auf die Lösegeldforderung einzutreten.**

Waterhole: **Methode, um eine Zielgruppe, wie die Mitarbeiter eines Unternehmens, zu infizieren. Die Angreifer spüren Websites auf, die Mitglieder der Zielgruppe öfter besuchen. Eine dieser Seiten wird mit einer Schadsoftware infiziert, sodass diese Software beim nächsten Seitenbesuch auf die Rechner der Zielpersonen übertragen wird.**

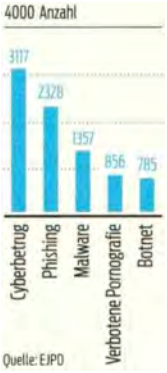
Cyber-Abwehr

Der Analyst
Pascal Lamia leitet die Meldestelle Melani, die Unternehmen hilft.

Der Strafverfolger
Stephan Walder ist Co-Leiter des Zürcher Kompetenzzentrums Cybercrime.

Vorsicht Betrug

Meistgemeldete Cybercrimes in der Schweiz



Boombranche

Verdachtsmeldungen per Online-Meldeformular in der Schweiz

Datacrime-Land Schweiz

Polizeilich registrierte Straftaten in der Schweiz

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG
ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch