

Wik

Zeitschrift für die Sicherheit der Wirtschaft

Sabotageschutz:
**Bilanz: SÜG
hat sich meist
bewährt**

Seite 10

Ermittlungspraxis:
**Besser auf den
Staatsanwalt
vorbereiten**

Seite 20

Neue Richtlinie:
**Fluchtwege
künftig behin-
dertengerecht**

Seite 45



ORGAN:
ARBEITSGEMEINSCHAFT
FÜR SICHERHEIT DER
WIRTSCHAFT e.V. - ASW

Zentralorganisation der Wirtschaft

**ASW-Ausbildungstagung:
Bestandsaufnahme und Analyse**
Aus den regionalen Sicherheits-
verbänden

Kriminalprävention im Finanzsektor
**Polizei: SB-Service
verlagert Risiken zu
den Kunden**

Seite 13

IT-Gefährdungen

Viren verursachen Schnupfen, das trojanische Pferd ist ohnehin nur eine von Homer erfundene Überlieferung und Malware vielleicht ein Anglizismus für Buntstifte? Zumindest im deutschen Mittelstand gibt es noch eine ganze Reihe von Entscheidungsträgern, denen die IT-Sicherheit absolut gleichgültig ist oder vernachlässigenswert erscheint. Gerade hat das



auch wieder das „International Security Barometer“ von Panda Security belegt: 14% der befragten deutschen Unternehmen haben nichts im Einsatz, was ihre IT schützen könnte. Doch mindestens genauso bedenklich ist, dass die anderen 86% vermutlich glauben, dass sie allein schon deshalb sicher seien, weil sie eine Sicherheitslösung nutzen. Unser Gesprächspartner in dieser WIK, Gunnar Porada, einer der es zum Beruf gemacht hat, die Lücke im IT-Sicherheitskonzept zu finden, meint jedenfalls, es sei in der Regel „kinderleicht“ ein Unternehmen zu hacken und

zu schädigen (Seite 29).

IT-Laien unter den Security-Experten, die das wohl nicht als leicht, sondern als hochkomplex und kaum erklärbar ansehen, hilft vielleicht das Wissen, dass es all die Gefährdungen, mit denen sie sich in der klassischen Sicherheit beschäftigen, in vergleichbarer Weise und ebenso real in ihren Auswirkungen auch im Netz gibt. Es gibt Diebstahlsdelikte, Betrug, Vandalismus, Spionage, Sabotage, Fälschungen, üble Nachrede oder Erpressung. Auch bei der Abwehr vieler Deliktformen in der digitalen Welt lassen sich Analogien zur realen Welt ziehen: Es geht vor allem darum, Unbefugten den Zugriff auf Hardware und Daten zu verwehren. Dies ist in der Datenwelt der Informations- und Kommunikationstechnik allerdings deutlich anspruchsvoller als bei einem realen Firmengelände. Reicht am Perimeter ein geschulter Wachmann in der Pforte oder vor dem Monitor der Leitstelle aus, um eine Intervention auszulösen, bleiben clevere digitale Angriffe für alle, die sich nicht intensiv mit der IT-Sicherheit befasst haben, unsichtbar.

Unser Trost: Auch Informatiker können das Problem der IT-Kriminalität nicht alleine lösen. Das Wissen um Täter und Motive ist genauso wichtig wie das um die digitalen modi operandi. Ein „Gefühl“ für das jeweils ergänzende Aufgabengebiet ist deshalb verzichtbar. Für SecuMedia war dieser Brückenschlag schon immer ein Anliegen. Aktuell haben wir dazu für unsere Abonnenten das gemeinsam mit unserer Schwesterzeitschrift <kes> und „IT-Grundschutz“ erstellte Special „Sicherheit im Rechenzentrum“ beigelegt*. Und wer nicht nur Schriftliches sucht: Im von SecuMedia organisierten „Themenpark IT-Security“ auf der SECURITY in Essen (5.-8.10.) oder auf unserer IT-Sicherheitsmesse it-sa in Nürnberg (19.-21.10.) bietet sich die Gelegenheit IT-Security-Experten direkt anzusprechen.

Horst Schäriges, Redaktion
redaktion.wik@secumedia.de

*Alle anderen Leser können es gerne (kostenlos) im Verlag anfordern:
vertrieb@secumedia.com



WISAG verbindet Sicherheit mit Service und umgekehrt

Als Prozessdienstleister verknüpfen wir Sicherheits- und Servicedienste ganz nach Ihren Anforderungen. So genießen Sie eine Rundum-Betreuung mit kurzen Abstimmungswe- gen. Das spart Geld und lässt Sie ru- hig schlafen. Profitieren Sie von dem Know-how eines der größten Dienst- leistungsunternehmen in Deutschland.



- Werk- und Objektschutz
- Revierbewachung
- 24 Stunden Notruf & Service Center
- Sicherheitstechnik
- Empfangs- und Telefondienste
- Post- und Archivdienste
- Messe- und Veranstaltungsservice

WISAG 
Sicherheitsdienste

WISAG Sicherheitsdienste
Holding GmbH & Co. KG
Kennedyallee 76
D-60596 Frankfurt / Main
24 Stunden Notruf & Service Center:
0800 4480004
www.wisag.de

Gunnar Porada:

Wer schlau ist, leistet sich gut bezahlte Hacker...

Das Besondere am „Google-Hack“ war nur die öffentliche Wirkung. Experten gehen davon aus, dass Angriffe dieser Qualität mittlerweile tagtäglich geschehen – sie fallen nur nicht auf, denn Unternehmen und Organisationen machen es staatlichen und privaten Hackern viel zu leicht, meint Hacking-Experte Gunnar Porada im Gespräch mit WIK-Mitarbeiter Claus Schaffner. Poradas Urteil: Erfolgreich Hacken ist oft „kinderleicht“.

Der Spiegel zitierte im Januar diesen Jahres die amerikanische Zeitschrift „Christian Science Monitor“ anlässlich des „Google-Hacks“ mit den Worten: „Wer genau genug hinsieht, wird zu jedem gegebenen Zeitpunkt die Datenspuren von Hack-Attacken, Wirtschaftsspionage-Versuchen und auch staatlichen Cyber-Schnüfflern finden.“ Ist tatsächlich so gut wie jedes Unternehmen betroffen?

Gunnar Porada: Das kann ich bestätigen. Diese Situation haben wir schon seit einigen Jahren und ich frage mich, warum immer noch so wenig für die Sicherheit getan wird. Der Schaden ist ja zweifelsfrei vorhanden, denn die Kriminellen verdienen damit viel Geld. Ich glaube, das Hauptproblem ist es, den Schaden im Einzelfall richtig zuzuordnen – was auch schwer ist, solange nicht gerade Kreditkarten geklaut wurden oder Angriffe so offensichtlich aufgefliegen sind, wie beim Google-Hack. Aber selbst dann ist es immer noch extrem schwer, alle Vorfälle zu rekonstruieren und zu beziffern.

Wenn ein Laie an IT-Sicherheitsmaßnahmen denkt, fallen ihm Malware-Scanner, Firewalls, Intrusion Detection, regelmäßige Updates und Awareness-Bildung ein. Ist er damit auf dem aktuellen Stand der Gefahrenabwehr?

Gunnar Porada: Auf dem aktuellen Stand der Masse auf jeden Fall. Und genau darum haben es die Angreifer so leicht, denn es ist viel zu wenig. Immer wieder stehen Fälle von Jugendlichen in der Zeitung, weil sie selbst große Unternehmen gehackt haben. Das sind keine Wunderknaben, sondern es ist eben immer noch „kinderleicht“ Firmen erfolgreich anzugreifen.



Gunnar Porada ist Geschäftsführer der inno-Sec GmbH und blickt auf nahezu 20 Jahre Erfahrung als Unternehmensberater im Bereich IT-Sicherheit zurück. Bekannt wurde er unter anderem durch Live-Hacking-Vorträge und die Demonstration von Sicherheitslücken beim elektronischen Reisepass und bei Online-Banking-Portalen. Aktuell entwickelt er einen Sicherheits-Browser („FireCastor“) der drive-by-Infektionen und infizierte pdf-Dateien abwehren soll.

Angenommen ein Unternehmen schafft es, „Schrotschuss-Angriffe“ von Cyber-Kriminellen ohne nennenswerte Schäden zu überstehen, mit welchen Angriffszielen oder Tätern muss es bei gezielten Angriffen auf die eigene IT rechnen?

Gunnar Porada: Den typischen Angriff gibt es nicht aber die Täter müssen sich meist auch nicht besonders anstrengen, um zum Ziel zu kommen. IT-Security wird in vielen Fällen missverstanden und oftmals ist einfach ein zu geringes Know-how vorhanden. Allein der Trugschluss, dass ein Virenschutzprogramm alle oder viele Viren abhält, ist fatal. Natürlich braucht jeder ein sol-

ches Programm, aber sie alle erkennen nur einen Bruchteil der Bedrohungen. Es ließen sich dann weitere Sicherheitsmechanismen einsetzen doch genau hier ist bei den Unternehmen oft schon Schluss. Diese Beispielsituationen gibt es auch in wesentlich komplexeren Fällen, wie beispielsweise im WAF-Umfeld (Web-Applikation-Firewalls) diese werden oft nicht richtig scharfgeschaltet. Ich habe auch schon einige Banken gesehen, bei denen dies der Fall ist. Dann wird ein gezielter Angriff recht leicht.

Regelmäßige Penetrations-Tests machen ebenfalls nur die wenigsten Unternehmen und wenn, dann nur um den „Report“ zu erhalten, etwa für die Kreditbeantragung. Danach passiert dann monatelang wieder nichts – in dieser Zeit entstehen aber Hunderte neue Angriffsmöglichkeiten, die Angreifer in rasender Geschwindigkeit ausnutzen.

Allerdings: Ein Patentrezept zum Schutz gibt es nicht. Den Aufwand für den Angreifer erhöhen hilft – und das ist ja auch das Ziel vieler Unternehmen. Die Umsetzung ist jedoch oftmals unzureichend. Grundsätzlich ist es auch hilfreich, die Angriffsmöglichkeiten zu minimieren. Nicht jeder „Spielkram“ ist wirklich notwendig, nur weil es gerade hip ist, ein schickes Telefon zu haben oder „wichtige“ E-Mails am Flughafen zu lesen. All diese netten Gadgets eröffnen den Angreifern wieder neue Möglichkeiten. Die Verantwortlichen in den Unternehmen wissen das meist auch, aber oft werden sie einfach überhört. Wenn dann aber der Schadensfall eintritt, will es keiner gewesen sein oder gar verantworten. ▶

Neo's Lettland-Hack

Laut BBC hat Anfang des Jahres ein Hacker unter dem Pseudonym Neo als Mitglied einer Gruppe namens „Fourth Awakening People's Army“ in Lettlands Regierung und Banken Daten zusammengetragen, die unter anderem belegten, dass die im Zuge der Bankenkrise bei Bankmanagern versprochenen Gehaltskürzungen meist nicht eingehalten wurden. Herausgestellt habe sich weiter, dass sich auch staatliche Unternehmen, die zur gleichen Zeit um finanzielle Unterstützung nachgefragt hätten, unzulässige Bonus-Zahlungen geleistet hätten. Betroffen waren rund 1.000 Unternehmen.

Nach Medienberichten sollen die Hacker über mehr als 7 Mio. vertrauliche Dokumente aus Regierung und Unternehmen verfügen, möglicherweise nicht nur aus Lettland.

Hätte eine Schweizer Bank eine Chance, die Identität deutscher Steuersünder wirksam vor kriminellen oder staatlichen Hackern zu schützen?

Gunnar Porada: Diese Frage würde ich mit einem „Ja“ beantworten. Es ist aber ein Wettrennen, das immer nur für einen bestimmten Zeitraum gewonnen werden kann. Sicherheit ist ein Prozess und hier ist Geschwindigkeit gepaart mit Know-how der Schlüssel zum Erfolg. Beim Know-how geht es aber schon los: Erworbenere Zertifikate, die die persönliche Kompetenz belegen sollen, sind in der IT-Security-Welt oftmals nicht mal das Papier wert, auf dem sie stehen. Und nur weil jemand mit der Technik umgehen kann, muss noch lange kein Sicherheitsdenken vorhanden sein oder umgekehrt. Die Kombination aus beidem ist leider selten, wäre aber sehr wichtig.

Manchmal spielen Zeit und Geld keine besondere Rolle – denken wir an staatlich unterstützte Lauscher, Hacker und Saboteure. Gibt es auch hier Schutzmöglichkeiten?

Gunnar Porada: Auch hier würde ich noch vorsichtig „Ja“ sagen, wobei die Technik hier die Schutzmöglichkeiten grundlegend eingeschränkt. Denn um gegen staatliche Angriffe sicher zu sein, ist es natürlich wenig hilfreich, Produkte aus den entsprechenden Ländern an sensiblen Stellen einzusetzen. Es ist ein

offenes Geheimnis, dass diverse Produkte mehr „machen“ als angegeben und gerne für diese Zusatzleistungen missbraucht werden. Das passiert immer häufiger und oft auch recht plump, weil kaum jemand darauf achtet. So gab es beispielsweise Fälle, wo chinesische Netzwerkgeräte – auch im engeren Umfeld der US-Regierung – in die Heimat gesendet haben. Und heute verbindet sich doch fast jedes Smartphone beim Synchronisieren mit irgendwelchen Online-Servern aber kaum jemand weiß genau warum.

Aber trotzdem kann durch richtige Mechanismen dafür gesorgt werden, dass auch fremde Regierungen einen zu hohen Aufwand haben. Es genügt schon „nicht mitzuspielen“ und eigene Produkte zu entwickeln, wie es beispielsweise China rigoros macht. Das kann sowohl im Großen wie auch im Kleinen sehr hilfreich sein. Für einen Angreifer egal ob staatlich oder zivil bedeutet es den größtmöglichen Aufwand, wenn er die Technik und die Mechanismen dahinter nicht kennt. Er muss dann anfangen zu probieren, das kostet wertvolle Zeit, die ihn den Wettlauf verlieren lässt.

Bei Militär, Forschungseinrichtungen, Regierungsstellen oder Kritischen Infrastrukturen wird die Abtrennung von offenen Netzen als Königsweg der IT-Sicherheit angesehen. Ist das zutreffend? Lässt sich das überhaupt durchhalten?

Gunnar Porada: Ob das durchzuhalten ist, können wohl nur die Betroffenen sagen. Aber es ähnelt sehr der von mir zuvor beschriebenen Möglichkeit. Durch den Einsatz von Eigenentwicklungen kann die Trennung hier dann aber mehrdimensional erfolgen. Ein simples Beispiel ist die Nutzung eigener Verschlüsselungsalgorithmen, die den sicheren Datentransport in öffentlichen Netzen ermöglichen. So ergibt sich eine Trennung innerhalb des unsicheren Netzes. Doch es muss eine durchgehende Sicherheitskette gebildet werden. Es reicht nicht aus, nur die Verschlüsselung zu nutzen, wenn links und rechts alles „beim Alten“ bleibt und dem Angreifer offen steht.

Ihr Kollege Kaspersky hat in einem Inter-

view gesagt, dass „man in der Computerwelt sehr viel besser verdient, wenn man für die Bösen arbeitet.“ Ich schliesse daraus, dass es nicht nur für „White Hacker“ sondern auch für „graue“ und „schwarze“ Experten einen funktionierenden Arbeitsmarkt gibt. Wer sucht hier wen?

Gunnar Porada: Es gab kürzlich erst wieder ein Versuch, mich für kriminelle Handlungen anzuwerben – den ich natürlich nicht angenommen habe. Aber es stimmt, der kriminelle Markt verdient überdimensional mehr Geld und das auch viel leichter. Das ist auch innerhalb der IT so, wobei der moderne Hacker seine Spuren sehr leicht verwischen kann und auch die Taten selbst selten auffliegen.

Ebenfalls kommt hinzu, dass viele kompetente Leute es schwer haben, legal Geld zu verdienen. Ich selbst habe jahrelang keinen Job bekommen, trotz diverser Vorstellungsgespräche und umfangreicher Bemühungen. So geht es vielen Leuten in der IT-Security-Branche. Da ist die Verlockung doch sehr groß „einfach mal Geld durch illegales Hacken zu verdienen“ und sei es auch nur, um offene Rechnungen zu zahlen. Wie viele der Verlockung erliegen, weiß ich nicht, aber ich sehe diese Situation als eine große Gefahr für jene, die sich schützen wollen.

Auch gegen politisch motivierte Hacker, wie beim Banken- und Regierungs-Hack in Lettland (s. Kasten), scheint kein Kraut gewachsen...

Gunnar Porada: Neo scheint einer dieser Spezialisten zu sein, mit einer gesunden Portion Wut im Bauch. Sein Hack zeigt aber gleichzeitig, wie mächtig diese kompetenten Hacker sind und verdeutlicht die Schiefelage. Wenn die Unternehmen schlau sind, machen sie sich diese Leute zunutze und lassen sich von ihnen helfen. Bedenken sollten sie allerdings bei der Bezahlung, dass diese Experten helfen können, Schäden in Millionenhöhe abzuwenden. Eine Abspiegelung mit Niedriglöhnen kann da eher wieder einen Bumerang-Effekt auslösen.