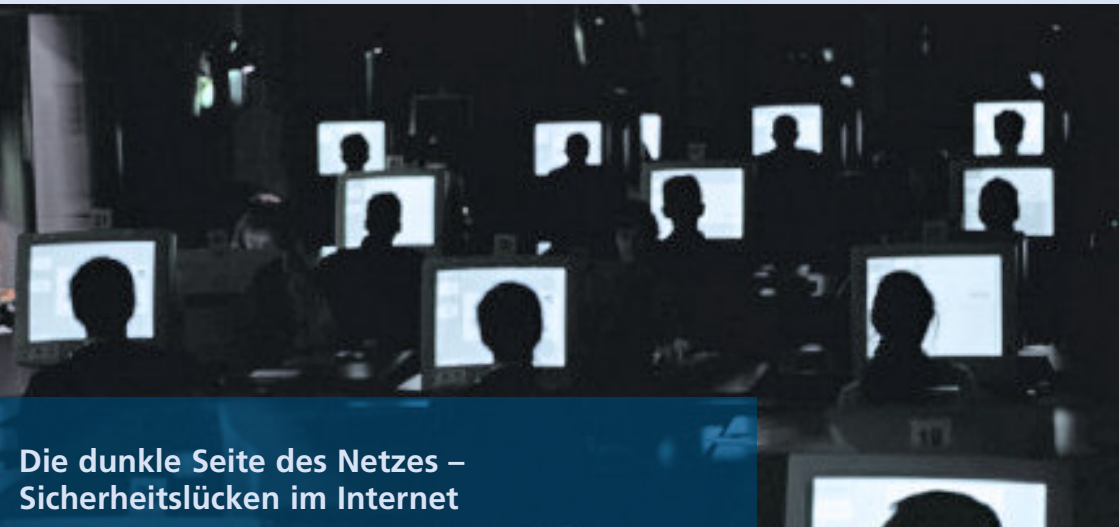




GASTVORTRAG
HAUPTVERSAMMLUNG



Die dunkle Seite des Netzes – Sicherheitslücken im Internet

Vortrag von Götz Schartner
anlässlich der Hauptversammlung der
R+V Versicherung AG am 06. Mai 2010



Im Finanzverbund der
Volksbanken Raiffeisenbanken

Vorwort

Kundendaten sind sensible Daten – jedes Dienstleistungsunternehmen weiß das. Gerade Banken und Versicherungen haben jeden Tag mit einer immensen Menge an personenbezogenen Daten zu tun. Der R+V Versicherung vertrauen 7,4 Millionen Kunden ihre persönlichen Informationen an. Bestmöglicher Schutz dieser Kundendaten ist oberste Priorität – bei R+V kümmern sich hoch spezialisierte Mitarbeiter um die Sicherheit der EDV-Systeme.

Die größte Gefahr droht heute aus dem world wide web, durch Virenangriffe auf Computer und EDV-Systeme. Diese Kriminalität aus dem Netz hat in den letzten Jahren stark zugenommen. Alle zwei Sekunden entsteht eine neue Variante eines Schadpro-

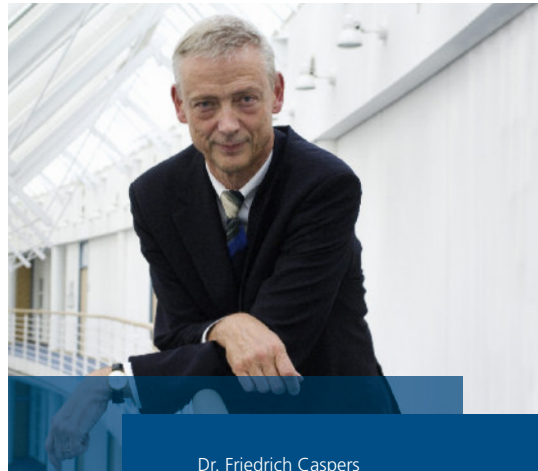
gramms, so das Bundesamt für Sicherheit in der Informationstechnologie (BSI). Und konnte sich ein Virus erst in einen fremden Rechner einschleichen, gibt es dem Täter einen nahezu vollständigen Zugriff auf den Computer des Opfers – oft unbemerkt.

Wie gehen kleine und mittlere Unternehmen, die sich keine eigene IT-Sicherheits-Abteilung leisten können, mit den Gefahren aus dem Netz um? Sind sie sich der Bedrohung überhaupt bewusst? Wissen sie, dass das Eindringen in fremde Netzwerke trotz Firewalls und Antivirenprogramme erschreckend einfach ist? Oft leider nicht, meint Götz Schartner, diesjähriger Gastredner auf der R+V-Hauptversammlung. Und er tut etwas dagegen: In zahlreichen Vorträgen vor

mittelständischen Unternehmen, vor Finanzdienstleistern oder auch Schulklassen leistet er Aufklärungsarbeit und sensibilisiert seine Zuhörer. Denn die Opfer von Angriffen aus dem world wide web sind eben nicht nur die großen internationalen Konzerne, sondern in der Mehrheit kleine und mittelständische Unternehmen – also klassische Kunden von Volksbanken und Raiffeisenbanken und R+V.



Dr. Friedrich Caspers
Vorstandsvorsitzender
der R+V Versicherung AG



Dr. Friedrich Caspers
Vorstandsvorsitzender der
R+V Versicherung AG



Kontakt:

Götz Schartner
8com GmbH & Co. KG
Donnersbergweg 1
67059 Ludwigshafen am Rhein

Tel. (06327) 976 428 – 0
Fax (06327) 976 428 – 99
E-Mail info@8com.de
www.8com.de

Der Referent

Götz Schartner wird häufig als professioneller Hacker im Dienste der Informationssicherheit bezeichnet: Im Auftrag von Unternehmen und als Auditor des Bundesamtes für Sicherheit in der Informationstechnik (BSI) schlüpft er in die Rolle von Cyberkriminellen, überwindet Sicherheitsbollwerke von Unternehmen und dringt so in fremde Netzwerke ein.

Im Jahr 2004 gründete Götz Schartner das IT-Security-Unternehmen 8com. Seitdem deckt Schartner gemeinsam mit seinen Mitarbeitern Sicherheitslücken in Unternehmensnetzwerken auf. Dabei verkaufen sie weder Hard- noch Software, sondern einzig und allein das eigene Wissen um die Schwachstellen von Sicherheitssystemen, deren Beseitigung meist keine großen Kosten verursacht.

Parallel dazu ist Götz Schartner auch in Sachen Aufklärungsarbeit viel unterwegs. In

seinen Vorträgen mit zahlreichen Live-Hacking-Demos zeigt er eindrucksvoll, wie leicht Datenklau, Bespitzelung oder das Abhören fremder Handys möglich sind. Seine Zuhörer sind vor allem mittelständische Unternehmen und Finanzinstitute, aber auch Kinder und Jugendliche, die er auf die Gefahren aus dem Netz aufmerksam machen möchte.



Irrtum Nummer 1 und 2:

„Wir haben eine hochwertige Firewall, uns kann nichts passieren.“

„Wir sind sicher, denn wir haben eine professionelle EDV-Abteilung.“

IT-Sicherheit und Cyberkriminalität: Die Gefahren aus dem Netz

Wer kennt schon die Gefahren aus dem Netz? Die meisten Unternehmen jedenfalls nicht. Gerade Unternehmen mit weniger als 500 Mitarbeitern glauben, dass sie einem geringeren Sicherheitsrisiko ausgesetzt sind, so der IT-Sicherheitsspezialist McAfee. Das Internet hat die weltweite Kommunikation erleichtert – macht gleichzeitig aber auch verwundbar. Das Risiko steigt, Opfer von Viren, Würmern oder Datendiebstahl zu werden.

Doch von vorne: Ohne IT – ohne Informationstechnologie – geht heute so gut wie gar nichts mehr. Informationstechnologien steuern schnell, zuverlässig und kostengünstig nahezu alle betrieblichen Prozesse. Große Mengen an Daten und Informationen werden digital gespeichert, verarbeitet oder weitergeleitet. Störungen innerhalb der IT, ein Verlust von Informationen, ein Verlust der Vertraulichkeit von Daten – eine Horrorvision für jedes Unternehmen.

Und: Selbst modernste Sicherheitstechnologie bietet oft keinen ausreichenden Schutz, denn Ziel der Attacken sind nicht die Stärken eines Systems, sondern dessen Schwachstellen.

Eine Firewall schützt Unternehmensnetzwerke nur bedingt. Antivirenprogramme sind oft unzuverlässig. Ein Mitarbeiter öffnet eine falsche E-Mail, schon schleicht sich der Schadstoff in seinen Rechner ein – und verbreitet sich von dort über das ganze Unternehmensnetzwerk. Kleiner Fehler – fatale Wirkung.

Oft macht es die Unkenntnis im Unternehmen den Cyberkriminellen besonders leicht, in fremde Netzwerke einzudringen. Aber auch große internationale Konzerne, die eine Menge Geld in ihre IT-Sicherheit investieren, sind vor Übergriffen aus dem world wide web nicht gefeit. Dazu die folgenden Beispiele.

Millionendiebstahl bei der CitiBank

Dezember 2009: Eine russische Gruppe hackt die CitiBank. Nach Informationen des „Wall Street Journal“ haben Hacker – Menschen, die in Computersysteme eindringen – ein IT-System der amerikanischen Citi-Bank geknackt und viele Millionen Dollar gestohlen. Die digitalen Bankräuber kamen offenbar aus Russland.

Über die angebliche Attacke sind nur wenige Details bekannt – die CitiBank dementierte den Vorfall. Offenbar wurde der Angriff bereits im Sommer 2009 entdeckt. Das FBI untersuchte den Vorfall, der zum Diebstahl einer mindestens zweistelligen Dollar-Millionensumme führte. Neben dem FBI waren auch der Geheimdienst National Security Agency und das US-Heimatschutzministerium eingeschaltet, um den Angriff zu kontern.

Dass Cyber-Gangster Geld stehlen, ist für amerikanische Sicherheitsexperten dabei nicht einmal das schlimmste Risiko. So sollen die Hacker neben der CitiBank auch eine US-Regierungsbehörde und andere Institutionen angegriffen haben. Die US-Sicherheitsexperten werteten die Tatsache, dass die Angreifer auch Daten manipulieren oder zerstören könnten, deutlich dramatischer als den Diebstahl von Geld. Das FBI schätzt den im vergangenen Jahr in den USA durch Online-Kriminalität verursachten Schaden auf eine Höhe von 260 Milliarden Dollar, umgerechnet 180 Milliarden Euro.



Irrtum Nummer 3 und 4:

„Wir haben doch Antivirensysteme, bei uns kommt kein Virus durch.“

„Warum sollte uns jemand hacken? Wir sind doch für niemanden interessant.“

Lautlos dringen hochspezialisierte kriminelle Hacker weltweit in professionell gesicherte Unternehmensnetzwerke ein und stehlen Daten. Besonders beliebt sind Kennwörter, Kreditkartennummern, Anmelde- und Nutzerdaten aus sozialen Netzwerken.

Hackerangriff auf Google

Januar 2010: Hackerangriff auf Google – obwohl das Unternehmen jährlich einen mehrstelligen Millionenbetrag in die IT-Sicherheit investiert. Google gehört damit zu den Firmen mit den besten Schutzfunktionen weltweit. Trotzdem haben es chinesische Hacker geschafft, in das Kernnetzwerk von Google einzudringen. Die Angreifer hatten es unter anderem auf wichtige Quellcodes von Programmen abgesehen. Ursache war eine Sicherheitslücke in Adobe Acrobat Reader. Der massive Hacker-Angriff aus China hatte auch auf 33 weitere amerikanische Firmen gezielt.

Hacker finden im chinesischen Internet übrigens alle möglichen Trojaner-Programme und andere Hilfen, um Computer auszuspionieren. Hacker-Training ist in China gar zu einer ganzen Industrie geworden. Die Größe des chinesischen Marktes für solche Cyberwerkzeuge wird offiziell auf eine Milliarde Euro geschätzt.

Betrugsangriff auf den Emissionshandel

Februar 2010: Phishing-Angriff auf die Computersysteme des Umweltbundesamtes. Kontoinhaber zahlreicher Emissionshandelsregister in Europa, Neuseeland und Japan haben Ende Januar 2010 gefälschte E-Mails erhalten. Es drohe eine Gefahr durch Hacker-Angriffe, hieß es darin. Diese Gefahr könne nur abgewendet werden, wenn sich die Nutzer neu registrierten. Absender der Mails schien die Deutsche Emissionshandelsstelle (DEHst) zu sein.

Wer den Verbrechern auf den Leim ging und die Aufforderung befolgte, gab seine Kontodaten auf einer Webseite preis, die dem Aussehen der Emissionshandels-Seite nachempfunden war. Insgesamt sieben der rund 2.000 Nutzer des deutschen Emissionshandelsregisters haben ihre Kontozugangsdaten weitergegeben und so den Betrügern den Zugriff auf ihre Konten ermöglicht. Damit konnten die Kriminellen in den Emissionshandel eintreten. Sie

übertrugen Emissionsrechte der getäuschten Firmen auf Konten vor allem in Dänemark und Großbritannien. Hier wurden sie allerdings nur kurz zwischengeparkt und dann weiterveräußert. Betroffen waren 250.000 Zertifikate. Aktueller Börsenwert: zwölf Euro pro Stück. Nach Informationen der „Financial Times Deutschland“ ist allein einem betroffenen Mittelständler ein Schaden von rund 1,5 Millionen Euro entstanden.



Cyber-Kriminelle sind weltweit aktiv und schwer zu fassen. Häufig ist es ein Kampf gegen Windmühlen: Fliegt eine Bande auf, taucht anderswo im Internet schon eine neue auf.

Eine globale Gefahr

Die organisierte Kriminalität hat heute weltweit ihre Geschäftsfelder auf die digitale Welt ausgedehnt. Digitale Raubzüge und Spionageangriffe gehören zu den am stärksten wachsenden Branchen – mit äußerst guten Profitchancen. Kriminelle erwirtschaften jährlich einen mehrstelligen Milliardenbetrag durch Datendiebstahl, Datenmanipulation und Erpressung – eine beliebte Zielgruppe sind auch kleine und mittlere Unternehmen in Deutschland.

Aber nicht nur Unternehmensnetzwerke werden attackiert. Auch private PC-Nutzer sind beliebte Angriffsziele. Einer BITKOM-Studie zufolge wurde bereits jeder zweite Deutsche Opfer von Kriminalität im Internet. Daneben gehört das Knacken von Handys, Blackberrys oder iPhones schon fast zur Routinearbeit der Kriminellen. Technisches Verständnis ist dafür nicht notwendig – die benötigten Programme kann man im Internet kaufen. Das Opfer muss nur auf

eine falsche MMS mit integrierter Spionagesoftware reinklicken und sie öffnen – schon können Kriminelle das fremde Handy komplett fernsteuern: Telefonate mithören, SMS und MMS verfolgen, Adressdaten einsehen – jetzt ist alles möglich.

Täter und Opfer

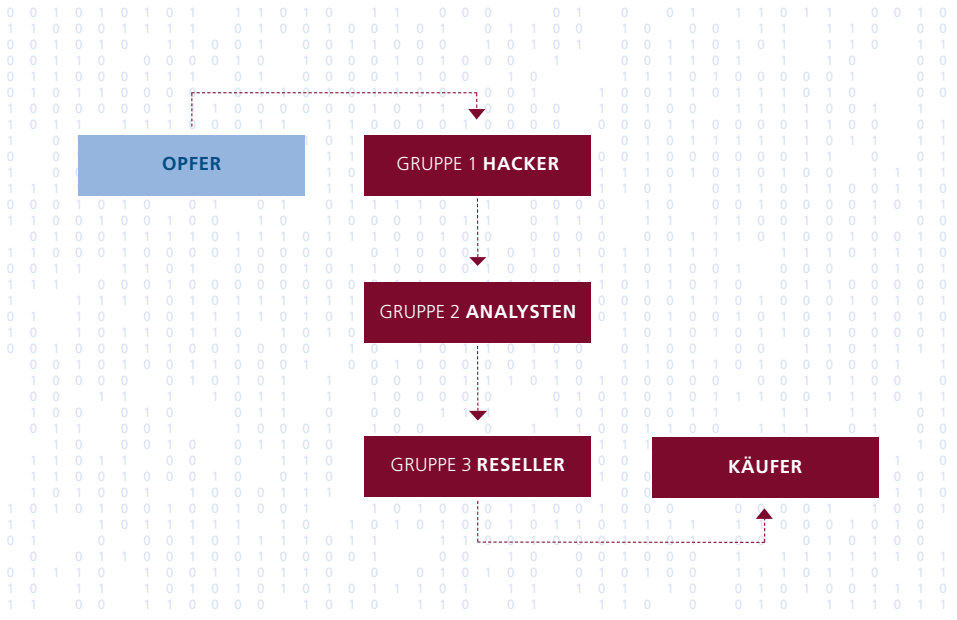
Die dunkle Seite des Netzes hat sich fest etabliert. Kein Wunder: Die Wachstumschancen sind immens. So immens, dass ganze Drogenkartelle in das Geschäft einsteigen; die Ertragsmöglichkeiten betragen ungefähr das 1.000-fache des Drogengeschäfts.

Wie arbeiten Cyber-Kriminelle?

Die Durchführung digitaler Straftaten ist heute technisch sehr einfach – und die Gefahr, gefasst zu werden, sehr gering. Die Kriminellen müssen nicht vor Ort agieren. Sie sitzen in Argentinien, Chile, China, Russland oder sonst irgendwo auf dieser Welt. In den seltensten Fällen werden sie strafrechtlich verfolgt. Sie können es sich in aller Ruhe gutgehen und ihre Geschäfte unbremst wachsen lassen. Hacker-Romantik? Das war einmal. Dahinter stecken schon lange keine Pizza essenden, experimentierfreudigen Jugendliche mehr. Die Verbreitung und Nutzung schädlicher Software folgt einem strikten Geschäftsmodell gut organisierter krimineller Gruppen.

Cyber-Kriminelle sind über den gesamten Globus verteilt und arbeiten absolut anonym. Mittlerweile haben sich richtige Dienstleistungsorganisationen im Netz etabliert. Meist handelt es sich dabei um perfekt strukturierte Organisationen, die aus mehreren, untereinander vernetzten Gruppen bestehen. Jede Gruppe ist in einem bestimmten Bereich hochspezialisiert, sucht sich eine Nische und verkauft ihre Produkte an Interessenten aus aller Welt.

Oft kennen sich die Beteiligten nicht einmal. Viele Mitglieder der Organisation sind – offenbar abgesehen von einem kleinen Kreis Eingeweihter – anderen Mitgliedern lediglich unter einer sogenannten ICQ-Nummer bekannt. ICQ ist ein Instant Messaging Programm: Benutzer können damit über das Internet miteinander chatten oder zeitverschoben Nachrichten versenden. Der Instant Messenger ist das verbreitetste Kommunikations-Tool unter den Cyber-Kriminellen.



Struktur der Cyber-Kriminellen:

Gruppe 1 – die Hacker:

Hacker sind diejenigen, die die Daten stehlen. Mit diesen Daten erpressen sie ihre Opfer. Hackergruppen greifen weltweit ungezielt Unternehmen an. Sie verschicken ein paar hunderttausend E-Mails mit infizierten Anlagen. Und wenn sie nicht selbst erpresserisch tätig werden, verkaufen sie die gestohlenen Daten an sogenannte Analysten-Gruppen weiter.

Gruppe 2 – die Analysten-Gruppe:

Sie schauen sich die Daten an, überlegen sich, an welchen Reseller sie die Daten weiterverkaufen können oder wie man damit sonst noch Geld verdienen kann.

Gruppe 3 – die Reseller:

Sie verkaufen letztendlich die Daten an den Endabnehmer.

Online-Schwarzmarkt

Im Internet existiert ein blühender Schwarzmarkt, in dem die verschiedensten Programme und Dienstleistungen angeboten werden. Das Waren-Angebot umfasst ganz verschiedene Arten von Daten. Es fängt an bei Name, Anschrift und Bankverbindung einzelner Personen und reicht bis hin zu Kopien ganzer Datenbanken von Online-Shops. Mit der Beliebtheit von social media Netzwerken stieg in den vergangenen Monaten auch die Nachfrage nach Benutzerdaten aus solchen Foren. Außer Listen von Daten kann man aber auch sogenannte Botnetze im Online-Schwarzmarkt kaufen. Ein Bot ist ein Computerprogramm, das selbständig sich wiederholende Aufgaben abarbeitet; ein Botnetz demzufolge ein Netzwerk aus mindestens einigen Tausend bis hin zu mehreren Millionen infizierter Computer, die ferngesteuert auf Aktionsbefehle warten. Kriminelle können damit Millionen von Spam-Mails versenden oder einen bestimmten Internetdienst mit so vielen Anfragen über-

schütten, bis er zusammenbricht. Der Versand von Spam-Mails ist übrigens nicht sehr teuer. Eine Million Spam-E-Mails kosten bei einem Botnetzbesitzer zwischen 250 bis 700 US-Dollar (ca. 200 bis 560 Euro). Ein eher kleines Botnetz mit rund 20.000 Computern benötigt für die Versendung von einer Million E-Mails bei zwei E-Mails pro Sekunde gerade mal 25 Sekunden.



Ob geklaute Kreditkartendaten, Ebay-Accounts oder Botnetze – Hacker verkaufen alles paketweise im Internet. Je vollständiger die Daten, um so wertvoller.

Spam-Attacke auf Facebook

Anfang des Jahres wurde der Internetdienst Facebook Opfer einer Botnetz-Attacke. Ende März 2010 starteten Online-Kriminelle einen massiven Spam-Angriff auf alle Facebook-Nutzer – mit einer ganz ähnlichen Masche wie bei dem bereits beschriebenen Emissionshandelsbetrug: Die Kriminellen versendeten E-Mails, in denen sie den Nutzer dazu aufforderten, sein Passwort aus Sicherheitsgründen neu einzugeben. Dazu müsse der Adressat nur den Anhang der Nachricht öffnen. Wer der Anweisung in der E-Mail folgte, lud sich jedoch verschiedene Schadprogramme und einen Passwortspion auf seinen Computer. Der Angriff richtete sich gegen die 400 Millionen Facebook-Mitglieder weltweit, darunter auch 7,6 Millionen deutsche Nutzer. Die Online-Kriminellen hofften dabei auf die Arglosigkeit der Nutzer. Sie sollten aus Angst um ihren Zugang zu dem weltweit beliebtesten Sozialen Netzwerk möglichst ohne Nachdenken auf den Anhang klicken.

Doch damit nicht genug – ein paar Wochen später las man folgende Schlagzeile: „Geklaute Facebook-Konten zum Schleuderpreis.“ Ein Online-Krimineller bot die Zugangsdaten zu 1,5 Millionen Facebook-Accounts bestehend aus Nutzernamen und dazugehörigem Passwort zum Kauf an – und das zu einem ungewöhnlich niedrigen Preis: Pro tausend Datensätze verlangte der Kriminelle umgerechnet etwa 20 bis 35 Euro – macht zwei Cent für ein einzelnes Nutzerkonto. 700.000 Datensätze waren da angeblich schon erfolgreich verkauft.

Was machen die Käufer mit solchen Daten? Sie nutzen die geklauten Facebook-Konten ebenfalls für Spammessages mit Links zu manipulierten Internetseiten. Besonders perfide: Die Nutzer klicken jetzt auf diese Mails, weil sie denken, ein Freund aus Facebook habe ihnen die E-Mail mit dem Link geschickt. „Gewöhnlicher“ E-Mail-Spam wird heute kaum mehr geöffnet. Dagegen

vertrauen viele blind den Nachrichten, die innerhalb der sozialen Netze wie Facebook verschickt werden – die Trefferquote für die Spammer ist hier also deutlich höher. Außerdem erbeutet der Käufer eines geknackten Nutzerkontos auch gleich alle mit dem Konto verbundenen Facebook-Freunde, deren Kontaktinformationen er dann ebenfalls für Spam-Nachrichten missbrauchen kann.

Wer sich im Internet bewegt, ermöglicht anderen den Zugang zur eigenen digitalen Identität. Dessen muss man sich bewusst sein. Gerade soziale Netzwerke werden gerne angegriffen. Welcher Nutzer rechnet damit, dass die Mail eines Freundes eine Bedrohung sein kann?



Gerade kleine und mittlere Unternehmen sind regelmäßig Opfer von Cyber-Attacken. Davon betroffen sind insbesondere die Gebiete Kundendaten, geistiges Eigentum und Kreditkartendaten.

Wer sind die Opfer?

Nicht nur große internationale Konzerne werden gehackt. Im Gegenteil: Besonders betroffen sind in Deutschland mittelständische Unternehmen. Mehr als die Hälfte der Schäden, die durch Spionage erwirtschaftet werden, geht zu Lasten der deutschen Mittelständler. Eine Studie der Münchner Beratungsgesellschaft Corporate Trust hat bestätigt, dass über 96 Prozent der Schäden auf kleine und mittelständische Unternehmen entfallen. Und fast ein Viertel der Schadensfälle belaufen sich auf mehr als 100.000 Euro, hat das Wirtschaftsprüfungs- und Beratungsunternehmen KPMG herausgefunden. Viel Geld für einen Mittelständler. Dazu zwei Beispiele: Ein Produktionsunternehmen aus Baden-Württemberg mit rund 100 Mitarbeitern erzielte bis 2008 etwa 30 Prozent seiner Neuaufträge in der Russischen Föderation. 2008 ging das Auftragsvolumen in der Russischen Föderation auf einmal massiv zurück: Es fiel auf rund zwei Prozent. Bei einer Überprüfung Anfang

2010 wurden Spionageprogramme entdeckt, die vor mindestens 2,5 Jahren ins Unternehmen eingeschleust worden waren. Die kompletten Rechnersysteme waren verwandt. So landete jede Ausschreibung, jedes Angebot des Unternehmens bei russischen Hackern, die die Informationen an Wettbewerber der Produktionsfirma weiterverkauft haben.

Eine Steuerberatungskanzlei aus Hessen mit 15 Mitarbeitern betreibt ihr Netzwerk selbständig. Eines Tages erhält der Steuerberater eine E-Mail aus Südamerika. Der Inhalt: Angeblich wurde das Unternehmensnetzwerk gehackt und alle Mandantendaten gestohlen. Spezialisten überprüften das Netzwerk und stellten fest, dass auf allen Computern der Kanzlei Fernsteuerungsprogramme installiert waren – und das bereits seit sechs Monaten. Damit konnten die Hacker jederzeit auf Kunden- und Finanzdaten zugreifen.

Ein paar Wochen später kam eine zweite Mail aus Südamerika. Der Absender verlangte jetzt die Zahlung von 100.000 Euro auf ein Konto in Argentinien – sechs Monate, nachdem die Spionageprogramme eingeschleust wurden. Der Grund: Vorher hätte die Kanzlei die Forderung von 100.000 Euro nicht zahlen können. Die Kriminellen hatten die finanzielle Situation der Kanzlei ganz genau überwacht und so lange gewartet, bis sie einen interessanten Mindestbetrag erpressen konnten. Zunächst weigerte sich die Kanzlei zu zahlen, aus Angst wiederholt Opfer einer Erpressung zu werden. Doch darauf waren die Hacker bestens vorbereitet. Sie nannten dem Steuerberater drei Referenz-Kanzleien, die sie ein Jahr vorher erpresst hatten. Und diese drei Kanzleien konnten bestätigen, dass sie nur einmal erpresst wurden. Hinter der ganzen Aktion steckte ein gut funktionierendes Geschäftsmodell organisierter Kriminalität.

Tipp

Bei Angriffen aus dem Netz sollten sich Unternehmen an den Verfassungsschutz wenden; der kümmert sich um die Verfolgung der Straftaten – ohne den Produktionsprozess im Unternehmen zu stören.



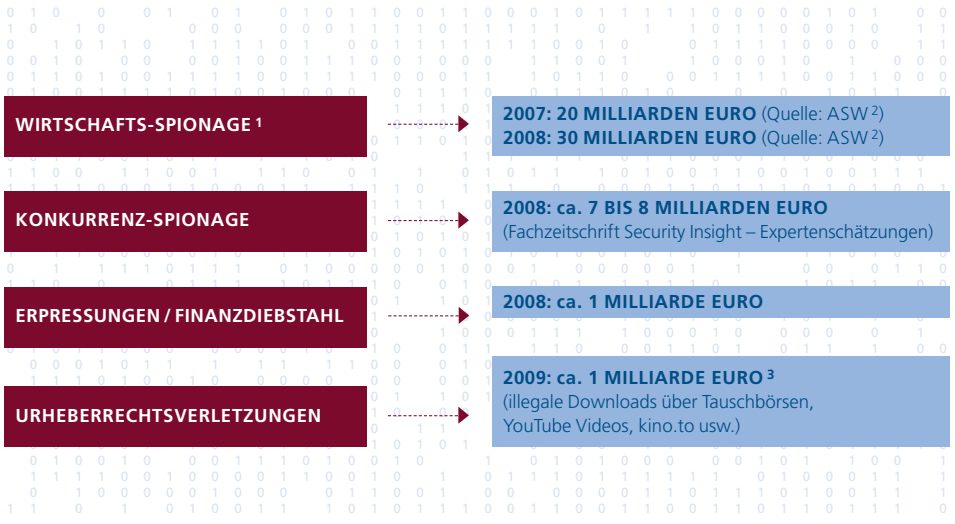
Vorsicht: Wer es Computerverbrechern leicht macht, muss für den Schaden haften. Da man den Verfasser eines Virus fast nie zu fassen bekommt, werden diejenigen in die Pflicht genommen, die den Virus verbreiten.

Schäden in Deutschland

Insgesamt 207.000 Taten mit dem „Tatmittel Internet“ hat es laut Bundeskriminalamt (BKA) 2009 gegeben, 30.000 mehr als 2008. Das genaue Ausmaß der Schäden zu beziffern ist sehr schwierig. Die folgenden Zahlen hat die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW) veröffentlicht, zum Teil sind sie hochgerechnet.

Tatbestand Wirtschaftsspionage: Laut Definition des Bundesamtes für Verfassungsschutz ist Wirtschaftsspionage staatlich gelenkt, geht von fremden Nachrichtendiensten aus und dient der Ausforschung von Unternehmen. Allein 980.000 Menschen arbeiten für den chinesischen Nachrichtendienst. Die Schäden aus Wirtschaftsspionage in der deutschen Wirtschaft sind enorm: Die ASW errechnete für das Jahr 2007 Schäden in Höhe von 20 Milliarden Euro, ein Jahr später bereits 30 Milliarden Euro.

Bei der Konkurrenzspionage ist kein Nachrichtendienst beteiligt: Eine Hackergruppe hackt ein Unternehmen und verkauft die erbeuteten Informationen an einen Wettbewerber. Die Fachzeitschrift Security Insight schätzt die Schäden in diesem Bereich auf sieben bis acht Milliarden Euro. Die Schäden aus Erpressung nach Finanzdiebstahl belaufen sich auf rund eine Milliarde Euro.



¹ Definition laut Verfassungsschutz: Spionage durch ausländische Nachrichtendienste

² Arbeitsgemeinschaft für Sicherheit in der Wirtschaft

³ hochgerechnete Zahlen nach Erhebung von Verbraucherzentralen

Anzahl der Schäden laut Bundesamt für Sicherheit in der Informationstechnik (BSI):

Im Jahr 2009 stiegen die Fälle der Kriminalität in der Informations- und Kommunikationstechnologie um rund 33 Prozent auf 50.250 Fälle an. Größte Straftatengruppe: Computerbetrug mit einem Anteil von 46 Prozent (dazu gehören Online-Betrug in eCommerce-Portalen oder das sogenannte Phishing beim Onlinebanking). Auch beim Ausspähen/Abfangen von Daten wurden im vergangenen Jahr 11.500 Straf-

taten erfasst – ein Anstieg um 49 Prozent im Vergleich zum Vorjahr. Bei „Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten“ waren es 7.200 Fälle (plus 37 Prozent), gefolgt von „Datenfälschung, Täuschung im Rechtsverkehr bei Datenverarbeitung“ mit 6.300 Delikten (plus 11 Prozent).

Schutz: Was hilft wie viel?

Was also tun gegen die dunkle Seite des Netzes? Vollkommener Schutz ist nicht möglich: Die Täter passen sich veränderten technischen Gegebenheiten sehr schnell an und zeigen enorme Innovationsfähigkeiten. Cyberkriminelle greifen über seriöse Websites Computer an, Schadstoffe verborgen sich vor Schutzprogrammen und verändern ihre Muster selbsttätig.

Was leisten Antivirenprogramme? – Ein Selbsttest

Natürlich bieten Antivirenprogramme einen gewissen Grundschutz, leider aber auch nicht mehr. Die Sicherheitslücken von Antivirenprogrammen lassen sich durch folgendes Experiment sehr gut darstellen: Auf www.virustotal.com, einer Website eines spanischen Internetanbieters, sind 40 unterschiedliche Antivirenprogramme zusammengestellt. Nutzer können dort verdächtige Dateien prüfen lassen. Ein Beispiel: Beim Testdurchlauf wird ein Virus von allen 40

Antivirenprogrammen als gefährlich erkannt. Das Problem: Hacker verändern einen Virus, bevor sie ihn herumschicken. Wird nur ein kleines Detail in der Textausgabe verändert, schon zeigt sich folgendes alarmierende Ergebnis bei der Überprüfung auf www.virustotal.com: Von den 40 Antivirenprogrammen erkennen jetzt nur noch fünf, dass es sich hier um einen Virus handelt. Hacker verändern Viren so, dass sie von keinem Programm mehr erkannt werden.

Firewalls – was bringen Schutzmauern?

Standardmäßig sind Unternehmensnetzwerke durch Firewalls geschützt. Als Brandschutzmauer schützen sie das Unternehmensnetzwerk vor fremden Zugriffen aus dem Internet.

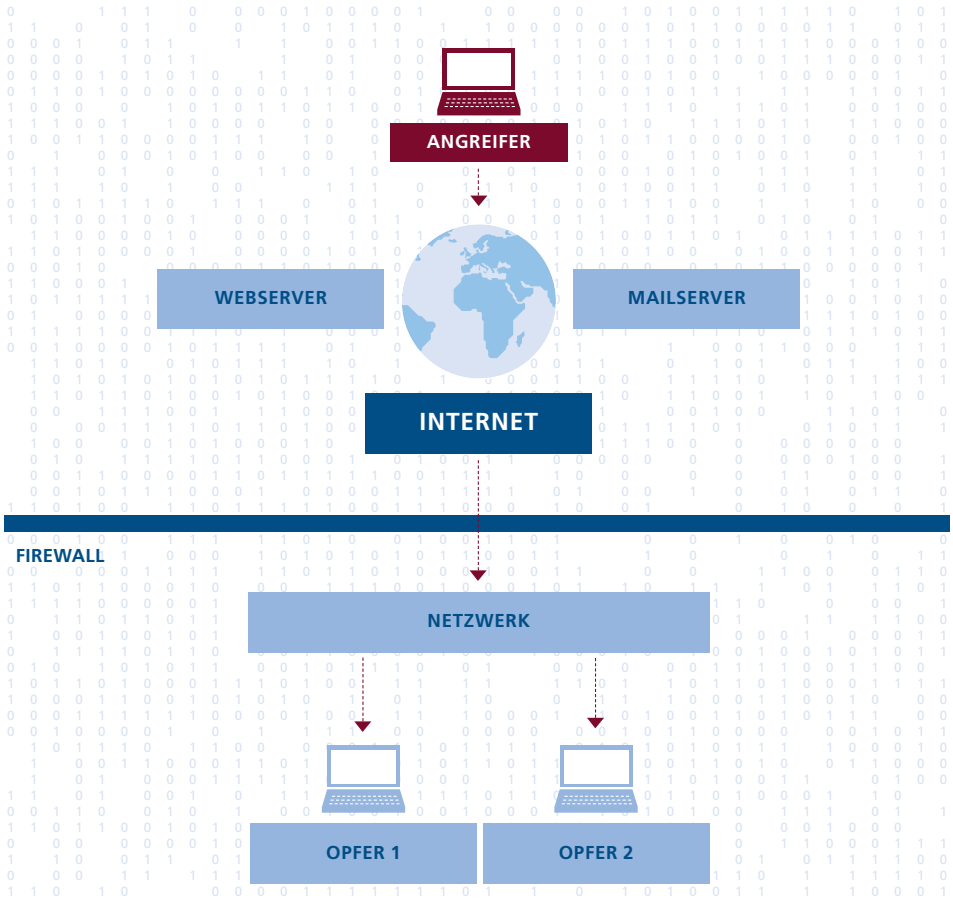
Doch trotz Firewall schleichen sich Hacker immer wieder von außen in das interne Netzwerk eines Unternehmens ein. Klingt

kompliziert – ist es meist nicht, denn die Vorgehensweise ist recht simpel: Zuerst suchen die Angreifer sich gezielt ein Opfer innerhalb eines Unternehmen aus. Das geschieht häufig mit Hilfe sozialer Netzwerke wie Xing oder Facebook. Dort findet man zahlreiche Unternehmen samt ihrer Mitarbeiter. Die meisten Mitarbeiter zeigen hier sogar ganz offen ihre Kontakte. Das Internet ist ein offenes Buch – herauszufinden, wer wen warum und wodurch kennt, ist sehr einfach. Diese Informationen nutzen Kriminelle.

Das Opfer erhält nun eine E-Mail von einem angeblich Bekannten aus Xing. Die Mail ist in allen Details perfekt: Anrede, Sprachstil, Betreff, Signatur – nichts erweckt das Misstrauen des Empfängers. So öffnet er die Mail und er öffnet die PDF-Anlage.

Die derzeit gefährlichste E-Mail-Anlage ist das PDF-Dokument. Nichts auf der Welt

Firewalls, Proxyserver, IDS/IPS oder Antivirensysteme hindern Angreifer nur bedingt, in Firmennetze einzudringen. Wer digitalen Bedrohungen präventiv und sicher begegnen will, setzt auf ein professionelles Zusammenspiel zwischen Mensch und Technik.



hat einen so großen wirtschaftlichen Schaden in der IT und in Unternehmen angeordnet wie dieses Dokument. Dabei ist nicht das PDF an sich unsicher, sondern der Acrobat Reader. Er weist seit Jahren immer wieder massive Sicherheitslücken auf, die zwar immer wieder geschlossen werden – aber viele Firmen spielen die Sicherheits-Updates nicht oder zu spät auf.

Die PDF-Anlage in der gefälschten E-Mail enthält ein Schadstoff-Programm, das von der Antivirus-Software im Unternehmen nicht erkannt wird. Dieses Programm baut eine reguläre und legale Internetverbindung zum Computer des Hackers auf. Der Hacker installiert seinen Schadstoff tief in das Betriebssystem des fremden Rechners – und übernimmt so dessen vollständige Steuerung. Von diesem Rechner aus kann er jetzt auch alle anderen internen Computer des Netzwerkes angreifen. So einfach und primitiv sind Hackingattacken.

Doch: Wer sich das Risiko bewusstmacht, hat den ersten Schritt zu mehr Sicherheit bereits getan.

10 Tipps für mehr Sicherheit im Unternehmen

1. IT-Sicherheitsmanagement

In jedem Unternehmen sollte mindestens ein Mitarbeiter den IT-Sicherheitszustand aus rechtlicher und praktischer Sicht beurteilen können, aktuelle Bedrohungen beobachten und entsprechende Maßnahmen einleiten können.

2. Patchmanagement

Moderne Hackingangriffe nutzen Sicherheitslücken im Betriebssystem oder in der Anwendungssoftware von Computern aus. In der Vergangenheit gab es diverse Sicherheitslücken im Acrobat Reader der Firma Adobe. Betriebssysteme, Anwendungsprogramme und speziell Anwendungen von Adobe müssen deshalb stets auf dem aktuellsten Stand sein.

3. Benutzerrechtekonzept

Administrative Benutzer müssen besonders vorsichtig sein: Nicht im Internet surfen oder E-Mails empfangen.

4. Professionelle Firewalls

Unternehmen oder Selbstständige mit

schützenswerten Daten sollten für die Internetverbindung keinen DSL-Router, sondern eine dem Schutzbedarf angemessene Firewall verwenden. Die Konfiguration der Firewall muss regelmäßig professionell überprüft werden.

5. Professionelle Antivirus-Software

Eine professionelle Antivirus-Software ist ein Muss. Ausgewählte PCs sind regelmäßig mit einer Antivirus Boot CD zu prüfen, Antivirus-Signaturen mehrmals täglich zu aktualisieren.

6. Internet, Surfen und E-Mails

Mitarbeiter-PCs benötigen eine Virtualisierungssoftware, das Surfen im Internet erfolgt über ein virtuelles Betriebssystem, das in der Virtualisierungssoftware läuft. Die Virtualisierung schottet Server und Anwendungen zuverlässig voneinander ab.

7. E-Mails, Absender, Anlagen

Absenderadressen von E-Mails können gefälscht sein. E-Mail Anlagen nur dann

öffnen, wenn sicher ist, dass der Absender stimmt.

8. IT-Security Awareness

Das IT-Sicherheitsbewusstsein im Unternehmen ist zu fördern.

9. Herkunft von Software

Software unbekannter Herkunft ist tabu. Kriminelle bieten häufig im Internet kostenfreie Programme an, die mit Schadsoftware versehen sind.

10. Kabellose Datenübertragung

WLAN-Zugänge sind per WPA2 mit einem 63 Zeichen langen Kennwort zu verschlüsseln. Schnurlose Telefone können abgehört werden.

Impressum

Herausgeber:

R+V Versicherung AG, Konzern-Kommunikation,
Taanusstraße 1, 65193 Wiesbaden

Verantwortlich: Rita Jakli

Redaktion: Anke Sostmann

Grafik: Heisters & Partner,
Büro für Kommunikationsdesign, Mainz

Fotografie: Andreas Varnhorn, Bad Vilbel (S. 3)

Anja Schmidt-von Rhein, Frankfurt (S. 4)
getty (S. 6, S. 17), laif (S. 9, S. 12), plainpicture (S. 20, S. 23)

Druck: Raiffeisendruckerei, Neuwied

1. Auflage, August 2010

Weitere Informationen unter:

www.8com.de

www.bsi.de / www.bsi-fuer-buerger.de

www.bitkom.de

www.bka.de

www.buerger-cert.de

www.internet-sicherheit.de

www.sicher-im-netz.de

www.verfassungsschutz.de



www.ruv.de