

«Der Faktor Mensch wird in Unternehmen bei Sicherheitsfragen nach wie vor unterschätzt»

Der Netzguide wollte von Sicherheitsexperte Thomas Dübendorfer, Präsident des Vereins Information Security Society Switzerland, wissen, was aktuell für Sicherheitslücken im Internet existieren und was dagegen unternommen wird. Interview: Patrick Brazzale



Dr. Thomas Dübendorfer ist Präsident des Vereins Information Security Society Switzerland (ISSS).

Wo sehen Sie heutzutage die grössten Gefahren bei Sicherheitslücken im Internet?

Am meisten gefährdet bei Sicherheitslücken im Internet ist zweifelsohne das Endsystem. Die Computer bei Benutzern vor allem im Heimbereich sind oftmals schlecht gewartet. Das heisst, der Benutzer hat nicht die neusten Softwareversionen oder aktuelle Sicherheitstechnologien installiert. Problematisch sind dann vor allem Computer, die infiziert und die ganze Zeit am Netz sind. Heutzutage werden Computer häufig nicht mehr abgeschaltet, somit kann ein solcher Computer praktisch die ganze Zeit missbraucht werden.

Wie können diese Sicherheitslücken geschlossen werden?

Es gibt verschiedene Ansätze, wie man versuchen kann, diese Lücken zu schliessen. Erstens kann man das Bewusstsein beim Endbenutzer steigern. Dies ist jedoch nicht wirklich umsetzbar. Denn die Frage ist, wie kann man 1,4 Milliarden Internetbenutzer erreichen? Wenn man versucht, die Awareness zu steigern, dann erreicht man nur kleine Gruppen. Teilweise werden die Anweisungen dann sogar falsch umgesetzt. Eine weitere Variante ist, dass man den Endbenutzern die Technologie liefert, die Sicherheitslücken schliesst oder gar nicht entstehen lässt. So können zum Beispiel Betriebssysteme automatisch Updates downloaden und installieren. Für viele andere Produkte gibt es diese Möglichkeit jedoch nicht. Man kann sogar sagen, dass jeder Hersteller seine eigene «Update-Suppe» kocht. Der Benutzer ist somit überfordert, alle seine Programme auf dem neusten Stand zu halten. Kommt noch erschwerend hinzu, dass praktisch jedes Programm einen eigenen Updatemechanismus besitzt. Laut einer aktuellen Studie von Secunia müsste der durchschnittliche Heimcomputerbenutzer 75 Sicherheitsupdates von 22 verschiedenen Herstellern einspielen. Zudem erscheinen etwa alle fünf Tage neue Updates, die sofort installiert werden müssten. Eine klare Überforderung, da eine Automatisierung weitgehend fehlt. Hier ist die Softwareindustrie aufgefordert, bessere Updatemechanismen zu liefern. Die dritte Möglichkeit besteht darin, dem Endbenutzer standardmässig die richtigen Sicherheitstools mitzuliefern. Mit dem Betriebssystem kann zum Beispiel eine Antiviren-Software oder eine funktionierende Firewall mitinstalliert werden. Die sollten so eingestellt sein, dass sie beste Systemsicherheit liefern. Wenn man heute ein System kauft, dann ist in der Regel eine einfache Firewall vorhanden, jedoch kein Antiviren-Scanner mit laufenden Aktualisierungen der Virensignaturen über die ganze mehrjährige Einsatzzeit des Systems. Ein vierter Ansatzpunkt ist, die Provider in die Pflicht zu nehmen. Täglich werden grosse Mengen an Spammails verschickt. Diesen Spam zu filtern stellt für viele Provider eine grosse Herausforderung dar. Es sind Bemühungen im Gange, die-

se Herausforderung in Angriff zu nehmen. Beispielsweise hat Swisscom (Bluewin) vor kurzem begonnen, ausgehende Spammails zu filtern. Es wurden dadurch gegen 10 Millionen ausgehende E-Mails pro Tag als Spam identifiziert und abgefangen, was einer jährlichen Spammail-Flut von 375 Terabyte entspricht. In meinen Augen ist es notwendig, dem Endbenutzer die Sicherheitsfrage abzunehmen und die verschiedenen oben beschriebenen Player in die Pflicht zu nehmen. Auf diese Weise entstehen diverse Sicherheitslücken erst gar nicht.

Vor kurzem wurde publik, dass sich Botnetze gegenseitig bekämpfen. Wie kommt es dazu?

Es ist einfacher für einen Bot, ein bereits infiziertes System anzugreifen, da dieses System eine Schwachstelle hat. Der «Wert» eines Computers steigt übrigens auch, wenn nur ein Bot installiert ist.

Die kriminelle Organisation dahinter kann somit allein über den Computer verfügen. Dazu ist zu sagen, dass Botnetze zwei Funktionen haben können. Erstens können sie

als Ressourcen gebraucht werden. So kann die Rechenleistung, Speicherplatz oder Bandbreite für verschiedene missbräuchliche Zwecke angezapft werden. Zweitens kann ein Botnetz gebraucht werden, um Informationen von den verschiedenen infizierten Computer zu sammeln und weiterverkaufen. Der zweite Fall kommt häufiger vor.

Welche Rolle spielt der Faktor Mensch in Sicherheitsüberlegungen?

Jedes System ist nur so gut, wie der Mensch, der es bedient. Wenn zum Beispiel Mitarbeiter Passwörter verwenden, die einfach zu knacken sind, dann ist die Schwachstelle in diesem Fall der Mensch. Leider wird der Faktor Mensch in Unternehmen nach wie vor unterschätzt.

Wie hat sich die Rolle der «Hacker» geändert?

Zu Beginn waren es eher vereinzelte Personen, die auf Sicherheitslücken aufmerksam machen wollten. Dahinter standen weniger finanzielle Absichten, als die technische Herausforderung. Heutzutage sind es klar finanzielle Absichten. Gut strukturierte Organisationen schlagen gezielt zu. Die Tendenz dieser kriminellen Handlungen ist steigend. So haben sich gemäss einer Statistik des FBI die Kosten von Cybercrime in den USA von 2008 auf 2009 auf 560 Millionen Dollar mehr als verdoppelt. Ein zweiter Bereich, in dem Hacking eine wichtige Rolle spielt, ist Counter Intelligence. Dabei geht es vor allem um den Aufbau von organisierten Strukturen innerhalb eines Staates, die feindliche Spionage abwehren.

Cloud Computing ist im Moment ein Trendthema. Was bedeutet dies für Anwender sicherheitstechnisch?

Bei Cloud Computing, das eine Weiterentwicklung von Software-as-a-Service ist, ist der Anwender besser geschützt als bei internen Systemen. Ein gutes Beispiel ist die Updateverwaltung, die bei einer grossen Menge interner Systeme alles andere als unkompliziert ist. Bei seriösen Anbietern

von Cloud Computing werden Updates und Sicherheitslücken dagegen schnell geschlossen. Es kann aber eine gewisse Abhängigkeit zu einem Anbieter entstehen. Darum ist es wichtig, dass man die AGBs sehr gut liest und sich nur mit Unternehmen einlässt, die gewisse Standards einhalten. Auch ist es wichtig, dass Anbieter verschiedene internationale Vereinbarungen unterzeichnen. Ein wichtiger Punkt für europäische Firmen beim Umstieg auf Google Apps ist, dass Google für die Einhaltung der Safe-Harbor-Datenschutzbestimmungen zertifiziert ist. Bei Safe Harbor handelt es sich um eine Vereinbarung zwischen der Europäischen Union beziehungsweise der Schweiz und den Vereinigten Staaten, die es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln unter Einhaltung der europäischen Datenschutzrichtlinien.

Sie sind Präsident der Information Security Society Switzerland (ISSS). Was ist das Ziel und Zweck dieser Vereinigung?

ISSS ist ein Verein, der zum Ziel hat, Security Professionals in der Schweiz zu vernetzen. Wir befassen uns mit

technischen, organisatorischen, wahrnehmungsbasierten, risikoanalytischen, wirtschaftlichen, soziologischen, regulatorischen und juristischen sicherheitsrelevanten Aspekten der Informationsgesellschaft in Theorie und Praxis. So organisieren wir Events zu verschiedenen Themen oder wir machen Arbeitsgruppen, die sich mit einer Problematik auseinandersetzen. Der Mitgliederbeitrag ist extra tief gehalten, damit der Verein für jegliche an Security interessierte Personen wie zum Beispiel auch Studierende interessant ist. Wir sind zudem auch gut vernetzt mit anderen ICT-Verbänden wie zum Beispiel ICTSwitzerland und SwissICT. ■

«Die Tendenz dieser kriminellen Handlungen ist steigend. So haben sich gemäss einer Statistik des FBI die Kosten von Cybercrime in den USA von 2008 auf 2009 auf 560 Millionen Dollar mehr als verdoppelt.»

Zur Person

Dr. Thomas Dübendorfer hat an der ETH Zürich promoviert und arbeitet als Senior Software Engineer Tech Lead bei Google in Zürich im Bereich Security. Er ist Präsident der Information Security Society Switzerland, nebenberuflich als Dozent an der ETH tätig und Gutachter und Berater für Informatik und IT-Security.