DIE ANGST VOR DEM ANWENDER

Aktuelle Bedrohungspotenziale

Die Schweizer IT-Verantwortlichen haben einen neuen Gefahrenherd ausfindig gemacht. Nicht Malware-Schreiber und Hacker sind für die IT-Sicherheit am gefährlichsten, sondern der Otto Normalanwender. → VON JENS STARK

Er ist das Ziel zahlreicher Anekdoten und Witze in den IT-Abteilungen: der sogenannte DAU, der «dümmste anzunehmende User». Doch der unbedarfte Anwender ist nicht nur das Opfer von Spott und Häme, er wird auch als regelrechter Gefahrenherd wahrgenommen. Dies hat unsere diesjährige Swiss-IT-Befragung unter fast 600 leitenden IT-Persönlichkeiten klar gezeigt.

Demnach scheinen die Schweizer IT-Verantwortlichen den unbedarften Anwender richtiggehend zu fürchten. Eine Zweidrittelmehrheit (66 %) stuft deren Gefahrenpotenzial als «hoch» oder «sehr hoch» ein. Nur 14 Prozent sehen im unabsichtlichen Fehlverhalten ein sehr niedriges oder niedriges Risiko (Grafik 1). Als Detail am Rande sei noch vermerkt, dass gerade auf diese Frage überdurchschnittlich viele CIOs geantwortetet haben. Diese «unabsichtliche Fehlverhalten der Nutzer» wird von den CIOs und IT-Leitern insgesamt als höchstes Bedrohungspotenzial für Schweizer Unternehmen angesehen, noch vor technischen Gefahren wie Malware und Spam. Richtiggehenden Attacken wie den ansonsten so gefürchteten Hacker- und DDoS-Angriffen (Distributed Denial of Service) bescheinigen die IT-Verantwortlichen in den Anwenderunternehmen dagegen nur ein mässiges bis niedriges Gefahrenpotenzial (Grafik 2).

Während die IT also vor den unbeabsichtigten Fehlern der Anwender bibbert, scheint sie zumindest den guten Absichten der eigenen User und auch der Externen zu vertrauen: In böswilligem Fehlverhalten erkennen die Befragten ein deutlich geringeres Gefahrenpotenzial. So sehen nur 28 Prozent das «vorsätzliche Fehlverhalten der Nutzer» als hohes oder sehr hohes Risiko. Fast die Hälfte (49 %) erkennt darin nur ein niedriges oder gar sehr niedriges Gefahrenpotenzial. Noch mehr Vertrauen bringen die IT-Leiter den Externen entgegen. Deren «vorsätzliches Fehlverhalten» schätzen nur 20 Prozent der Antwortenden als hoch oder sehr hoch ein, während eine Mehrheit von 52 Prozent deren Schadenspotenzial als niedrig oder sehr niedrig bewertet.

KEIN ÜBERRASCHENDES ERGEBNIS

Das Ergebnis dieser Befragung im Rahmen der Swiss-IT-Studie überraschte weder Experten noch Betroffene. Dafür werden vor allem zwei Faktoren genannt. Zum einen hat der technische Schutz heutzutage ein sehr hohes Niveau erreicht. «Gegen Malware und technische Hackerattacken kann man sich mit relativ einfachen Massnahmen wie Virenschutz, Firewall, konsequentes Patching sowie mit Intrusion-Prevention-Systemen, Datenverschlüsselung und Mehrweg-Authentisierung relativ gut

BILD: KEYSTONE/GAETAN BALLY

Feuerwerksköpfe für Raketen stehen in der Hans Hamberger AG in Oberried, Kanton Bern, zur Montage bereit

schützen», meint etwa Christoph Baumgartner, CEO und Inhaber der Thalwiler IT-Security-Beratungsfirma OneConsult. Der Mensch sei dagegen kreativ und lasse sich nicht in ein Korsett zwängen. Ähnlich sieht dies Daniel Graf, Informatiksicherheitsbeauftragter des Bundes, und damit verantwortlich für die IT-Security der gesamten Bundesverwaltung: «Gegen das Fehlverhalten von Nutzern kann man weniger vorkehren als beispielsweise gegen Malware.»

Thomas Schlienger, Geschäftsführer von Treesolution, einem Spezialisten für IT-Security-Awareness-Kampagnen, sieht auch noch andere Gründe für das hohe Gefahrenpotenzial der Anwender: «Die Wahrscheinlichkeit, dass Benutzer einen Fehler machen, ist rein statistisch gesehen bedeutend grösser als die Wahrscheinlichkeit, Opfer eines Hackerangriffs zu werden.»

> «Gegen das Fehlverhalten von Nutzern kann man weniger vorkehren als beispielsweise gegen Malware»
>
> Daniel Graf, Informatiksicherheitsbeauftragter des Bundes

SENSIBILISIERUNG TUT NOT

Es wäre aber zu einfach, die Schuld dem unbedarften Anwender alleine in die Schuhe zu schieben. Vielmehr wird bei den Unternehmen Handlungsbedarf gesehen. Dabei sind sich die Experten allerdings uneins, ob Schweizer Firmen genug unternehmen, um die Security-Awareness ihrer Angestellten wirklich nachhaltig zu erhöhen. Für Wolfgang Sidler, Inhaber von Sidler Information Security und Präsident von InfoSurance, ist der Fall klar: Schweizer Firmen tun zu wenig. «Hier ist noch ein sehr grosses Potenzial vorhanden», meint er. Ginge es nach ihm, müssten Schweizer Unternehmen klar mehr Geld in die Ausbildung der Endanwender stecken. →

DER RICHTIGE UMGANG MIT GEFAHRENGUT WILL GELERNT SEIN. MITARBEITENDE MÜSSEN FÜR DIE RISIKEN SENSIBILISIERT WERDEN

Ein Arbeiter in der Produktionshalle der Swiss Steel AG, der ehemaligen Von Moos Stahl AG, in Emmenbrücke, Kanton Luzern

Dabei sind entsprechende Kampagnen nicht einmal sonderlich teuer. «Eine Sensibilisierung der Mitarbeitenden im Bereich Informationssicherheit kann auch mit wenigen finanziellen Mitteln, allerdings mit entsprechenden organisatorischen Massnahmen, wirkungsvoll und effektiv umgesetzt werden», merkt Sidler an. Folglich sei nicht immer eine gross angelegte Sicherheitskampagne notwendig. Dem stimmt auch Thomas Schlienger zu: «Wichtig ist, dass man kontinuierlich am Ball bleibt.» Schliesslich seien die Menschen vergesslich, und die Risikolandschaft verändere sich laufend.

Nicht alle Experten stellen der Schweizer Unternehmerschaft punkto Awareness-Kampagnen ein schlechtes Zeugnis aus. Für Hannes Lubich, Dozent für ICT-System-Management am Institut für mobile und verteilte Systeme der Fachhochschule Nordwestschweiz in Windisch und langjähriger IT-Security-Verantwortlicher, «tun Schweizer Firmen im Durchschnitt mehr als viele Firmen im Ausland». Ihm zufolge könnten die Eidgenossen den Vorsprung sogar als Wettbewerbsvorteil ins Feld führen – sofern sie diesen nur besser vermarkteten. Auch Candid Wüest, Security Response Engineer von Symantec, meint, dass Schweizer Firmen nicht grundsätzlich zu wenig für die Verbesserung des sicherheitsrelevanten Verhaltens der Anwender tun. Ihm zufolge bestehen aber grosse Unterschiede zwischen den einzelnen Unternehmen und Branchen. «Einige Firmen geben sich viel Mühe, ein Awareness-Programm zu etablieren», berichtet er. «Dies geht dann bis zu Erinnerungsplakaten in der Kantine.» Leider gebe es aber auch das Gegenteil, zum Beispiel «auch grössere Unternehmen, die warten, bis es zu spät ist und der Schadensfall eintritt».

Schriftlich oder mündlich festgelegte Sicherheitsregeln, auf neudeutsch Policys genannt, helfen ebenfalls dabei, die Mitarbeiter zu sensibilisieren. Doch die beste Policy nützt wenig, wenn sie nicht verstanden wird – oder so umfangreich ausfällt, dass sie niemand liest, geschweige denn verinnerlicht. Laut OneConsult-CEO Baumgartner sollte die Policy deshalb nicht von der IT-Abteilung oder vom IT-Security-Team formuliert werden, sondern nach Möglichkeit von einem abteilungsübergreifenden Projektteam. Denn nur ein solches kann sicherstellen, dass die aufgestellten Regeln auch von den Endanwendern, deren technisches Verständnis nicht zwingend dem der IT-Mitarbeiter entspricht, verstanden werden. «Wenn die damit betrauten Leute ihre Aufgabe ernst nehmen, sorgen sie dafür, dass das verwendete Vokabular möglichst nahe an der Umgangssprache liegt sowie die Gebote und Verbote möglichst unmissverständlich formuliert werden», rät Baumgartner.

ERFAHRUNGEN AUS DER PRAXIS

Das Feilen an der Policy war auch einer der Schritte, um die Security-Awareness in der Bundesverwaltung anzuheben. Hier habe man bereits 2009 ein knapp und kurz gehaltenes Sicherheitsleitbild formuliert, führt Daniel Graf vom ISB aus. Allerdings sei dieses nur für die einzelnen Projekte wichtig, an die Mitarbeiter versuche man dagegen eher über andere Massnahmen heranzukommen. Laut Graf haben sich dabei gewisse Instrumente als nützlich erwiesen, andere sind fehlgeschlagen. Woher er das weiss? Beim Bund werde die Wirkung der Kampagnen analysiert. «Die Schulung mit Web-based-Trainingsprogrammen über die Informationsschutzvorschriften haben zumindest teilweise gute Ergebnisse gebracht», sagt Graf. Andere Massnahmen seien dagegen auf Ablehnung gestossen. «In verschiedenen Verwaltungseinheiten wurden kleinere Kampagnen mittels Social Engineering durchgeführt», berichtet er. So sei versucht worden, mit Phishing-Techniken wie einer «gefälschten» E-Mail oder mithilfe von Telefonanrufen Passwörter auszuspähen. «Diese Kampagnen wurden von den Mitarbeitenden vielfach eher negativ wahrgenommen und zeitigten meistens nur kurze Effekte», so Graf.

Anhand der Erfahrungen hat man beim Bund dieser Tage eine neue, vielschichtige Kampagne lanciert. Einzelne Security-Themen

GRAFIK 1

GEFAHRENPOTENZIAL DURCH UNABSICHTLICHES FEHLVERHALTEN DER NUTZER

Deutlich mehr als die Hälfte der IT-Verantwortlichen in den Anwenderunternehmen schätzen die Gefahr durch unbeabsichtigtes Fehlverhalten ihrer Mitarbeitenden als hoch bis sehr hoch ein.

Quelle: IDC, CW 2011 (n = 568)

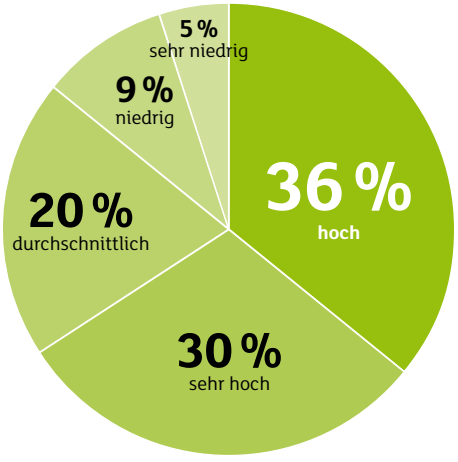
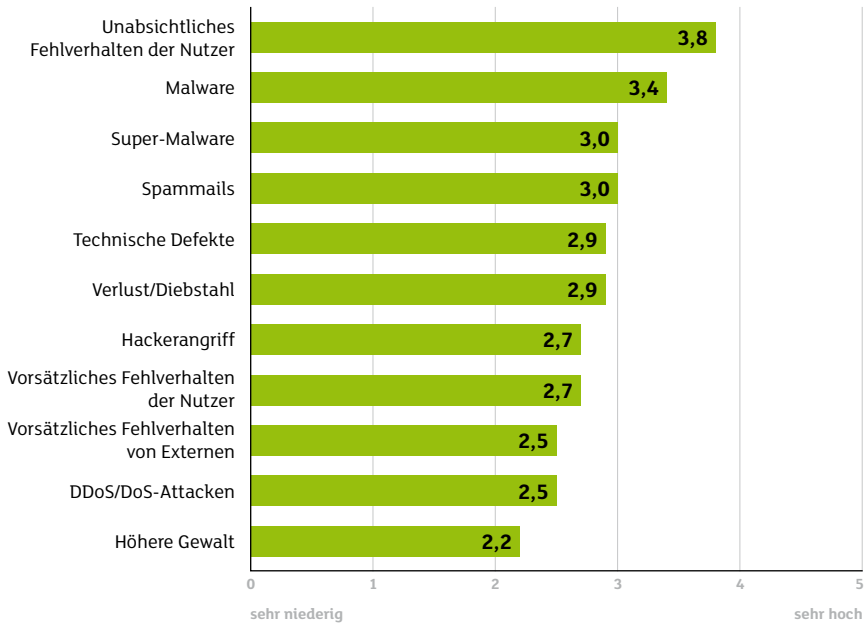


BILD: KEYSTONE/MARTIN RUETSCHI

GRAFIK 2

BEDROHUNGSPOTENZIALE IM BEREICH DER IT

Der unbedarfte User wird von der IT-Abteilung am meisten gefürchtet. Ihm wird ein höheres Gefahrenpotenzial zugeschrieben als jeder Malware- oder Hackerattack e. Quelle: IDC, CW 2011 (n = 568)



werden dabei monatlich im Intranet behandelt. Flankierend werben entsprechende Plakate für Aufmerksamkeit und ein Wettbewerb sorgt dafür, dass sich möglichst viele Mitarbeitende beteiligen. Dass die Informationssicherheit beim Bund Chefsache ist, beweist zudem eine Videobotschaft der zuständigen Bundesrätin Eveline Widmer-Schlumpf zum Thema, die ebenfalls im Intranet aufgeschaltet wurde.

Ein weiteres interessantes Awareness-Programm läuft derzeit an der ETH Zürich unter der Bezeichnung «safeIT». Wie Stephen Sheridan, Mitglied der Network Security Group der ETH und Projektleiter, berichtet, sprechen die einzelnen Massnahmen die verschiedenen Nutzergruppen wie Studenten und Mitarbeitenden unterschiedlich an. «Bei der jüngeren Generation haben wir gute Erfahrung mit kurzen Videos und Animationen gemacht», meint Sheridan. «Bei ihnen kommt auch die Verteilung von USB-Sticks gut an», ergänzt er. Bei den Mitarbeitenden sei dagegen die direkte Unterstützung und Schulung am effizientesten. Diese sei aber auch ressourcenintensiv und daher begrenzt.

DER FAKTOR MENSCH

Einig ist man sich, dass rein technische Mittel nicht ausreichen, um den Faktor Mensch in den Griff zu bekommen. «Technische Lösungen bringen natürlich einen gewissen Grundschutz, müssen aber durch organisatorische Massnahmen wie die Einführung des Mehraugenprinzips und einer strikten Gewaltentrennung sowie durch prozedurale Vorkehrungen wie Reviews und Audits ergänzt werden», schlägt Lubich vor – und warnt gleichzeitig vor zu restriktiven Systemen. «Schutzsysteme, die nahe an eine hundertprozentige Sicherheit reichen, wären für den Normalanwender so restriktiv, dass die Produktivität beeinträchtigt würde», gibt Lubich zu bedenken. Der Professor für ICT-System- & Servicemanagement krönt seine Argumentation mit einem Zitat von Isaac Newton: «Ich kann die Bewegung der Himmelskörper berechnen, aber nicht das Verhalten der Menschen.» ←