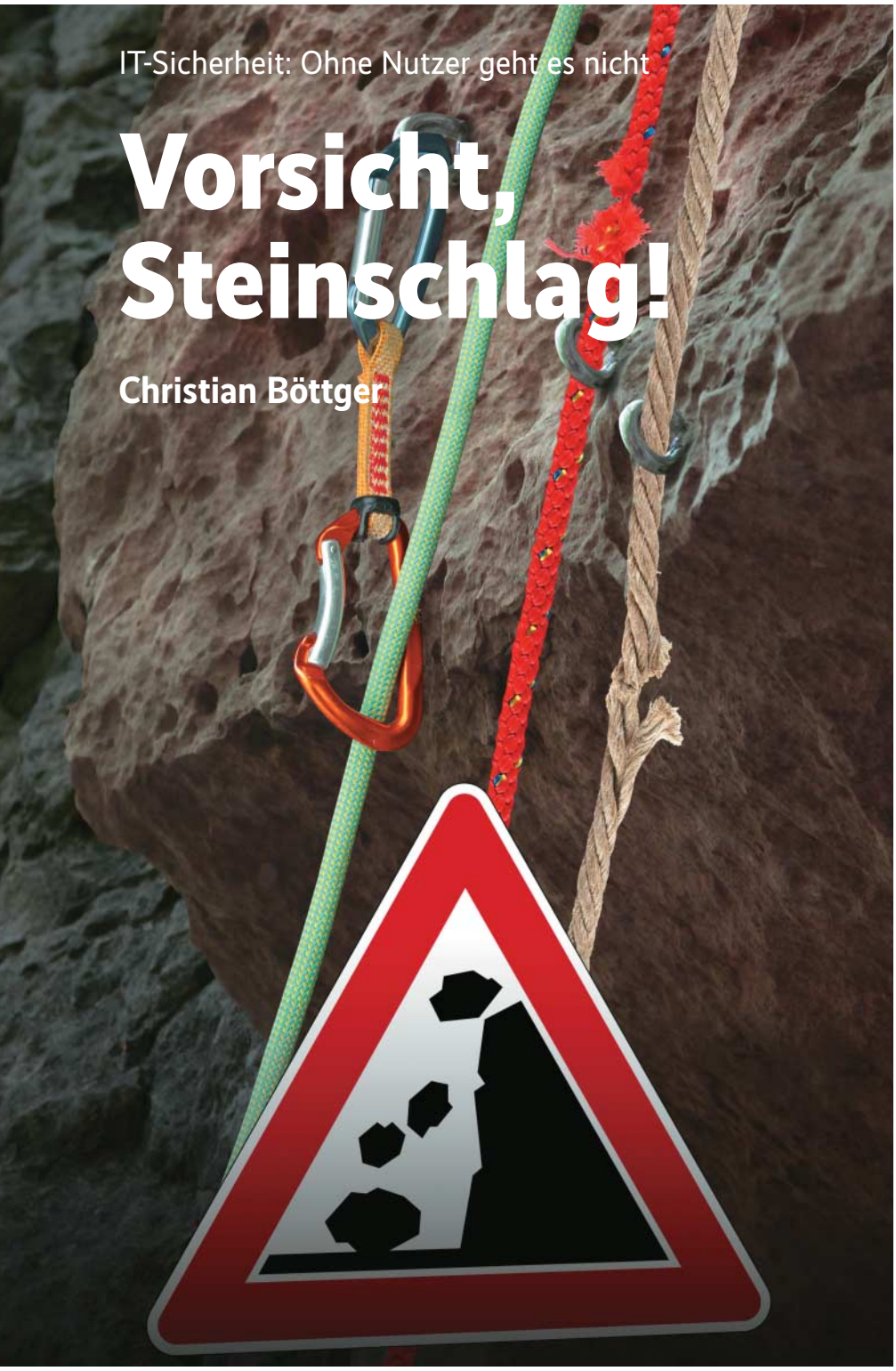


IT-Sicherheit: Ohne Nutzer geht es nicht

Vorsicht, Steinschlag!

Christian Böttger

Es ist immer dieselbe alte Leier: Das beste Sicherheitssystem nützt nichts, wenn man den Nutzer nicht mit ins Boot holt. Das zu bewerkstelligen, ist allerdings auch eine nie endende Aufgabe. Wie man sie anpacken kann, zeigt ein Projekt an der Universität Braunschweig.

IT-Sicherheit, oder besser Informationssicherheit, gilt immer noch als rein technisches Thema, nach dem Motto: „Das macht die IT-Abteilung“, und wenn man dort nachfragt: „Die Firewall betreut unsere Netzwerkabteilung.“ Lange Zeit war das sicherlich so und hat auch – mehr oder weniger – ausgereicht. Der Computernutzer in der Firma hatte damit nichts zu tun, außer dass er sich manchmal über das Antivirenprogramm ärgerte, weil dieser alles so langsam machte.

Zu Hause sah und sieht es kaum anders aus. Die Hersteller von Antivirenprogrammen suggerieren dem Nutzer, er müsse nur dieses eine Produkt kaufen und installieren, und schon sei er sicher. Seit einiger Zeit wird ihm auch eingebläut, dass er doch bitte immer sämtliche Software aktuell halten muss. Das stört den Benutzer aber kaum, denn inzwischen haben die meisten Softwarepakete eine Auto-Update-Funktion und Windows macht ohnehin alles selbst.

Im beruflichen Umfeld sollten sowieso alle Softwarewartungen zentral administriert und angestoßen werden. Von seinem Smartphone ist der Benutzer ja inzwischen auch gewohnt, dass es ständig irgendwelche Updates einspielt. Er fühlt sich vielleicht genervt, aber es gibt ihm auch das beruhigende Gefühl, dass sich jemand um die Sicherheit kümmert.

Also alles ganz einfach? Man ahnt es schon: Was so einfach aussieht, kann in Wahrheit nur zu einfach, das heißt zu kurz gedacht sein. Und genau so ist es. Es gibt keine „Sicherheit aus dem Regal“. Alle diese Maßnahmen sind notwendig und wichtig: Firewall, Antivirensoftware (obwohl es dazu inzwischen etliche abweichende Meinungen gibt) und Updates. Vollkommen unverzichtbar, ganz richtig. Nur leider nicht ausreichend.

Verlagerung der Waffen

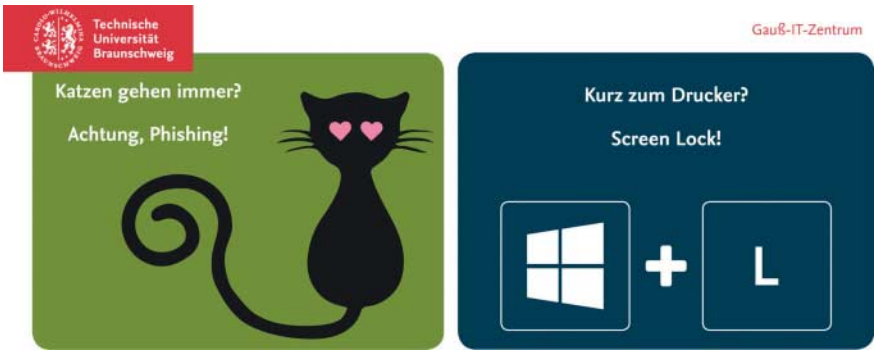
Gegen viele Angriffe kann und muss man sich auf technischem Wege schützen. Aber Technik alleine tut es nicht mehr. In Wahrheit hat sie es noch nie alleine getan, aber die Dimensionen werden immer größer.

Auf die technische „Aufrüstung“ auf „Verteidigerseite“ reagieren die Angreifer seit mehreren Jahren nicht mehr nur mit mehr und besserer Technik, sondern indem sie auf „weiche Ziele“ ausweichen. Deutlicher: Sie nutzen menschliche Schwächen aus, um über den Umweg „Nutzer“ an ihr Ziel zu kommen. Das vielleicht größte Sicherheitsrisiko sitzt vor dem Bildschirm an der Tastatur

oder hält ein Smartphone in der Hand. Auch dies ist nicht neu, letztlich ist es nichts anderes, als was Geheimdienste als HUMINT – Human Intelligence – schon seit Jahrtausenden betreiben, nur eben jetzt mithilfe moderner Technik aus der Ferne.

Die großen Massenangriffe, meist per sogenannter Phishing-Mail, zielen auf allgemeine menschliche „Urtriebe“: Angst („Klicken Sie hier, sonst ist Ihr Bankaccount gesperrt“), Gier („Klicken Sie hier und verdienen Sie 5000 Euro am Tag“ oder „hier klicken für das unglaublichste Schnäppchen Ihres Lebens“), Sex (nun ja, selbsterklärend) und gegebenenfalls noch den Spieltrieb („Katzenvideos gehen immer“). Manchmal wünscht man sich die „guten alten Zeiten“ mit Nigeria-Spam zurück, dieser war einfach zu erkennen. Die Phishing-Mails heute sind so gut gemacht, dass selbst Experten mehrfach hinschauen müssen, um sie zu erkennen.

Schlimmer noch: Immer mehr Angriffe werden genau auf eine Zielgruppe oder Institution zugeschnitten. Ein Beispiel ist eine groß angelegte Attacke, die gezielt Personalabteilungen angriff mit extrem gut gemachten, aber natürlich gefälschten Bewerbungen, die sich jeweils auf tatsächlich ausgeschriebene Stellen bezogen. Die per E-Mail zugesandten Unterlagen enthielten dann den Schadcode. Beliebt ist es auch, gefälschte Login-Seiten von Firmensystemen (meist Webmail) täuschend echt nachzubauen, mit einer auf den ersten Blick (fast) korrekten Adresse, und dann den Führungskräften ebenfalls gut gefälschte E-Mails zu schicken, mit der Aufforderung, sich dort einzuloggen. So gelangt der Angreifer frei Haus an die Zugangsdaten und kann nebenbei per „Drive-by“ auch noch Schadcode verteilen, wenn er möchte. Diese Methode des „Spear Phishing“ ist offensichtlich inzwischen so billig geworden, dass sie selbst gegen die Universität, an der der Autor tätig ist, mehrfach pro Jahr angewendet wird.



Viele Universitäten verfügen über Webseiten mit Informationen zur Sicherheit sowie Schulungs- und Sensibilisierungsmaterial. In der Regel sind diese für die Allgemeinheit zugänglich und nutzbar, etwa die hier gezeigten Mouspad-Vorlagen der TU Braunschweig (Abb. 1).

Gegen solche Angriffe kann man sich technisch kaum rüsten. Bevor Spear-Phishing-Mail erkannt wird, können bei einem großen Ziel wie einer Universität mit ca. 30 000 Mailkonten schon einige Hundert bis Tausend Mails zugestellt worden sein, bevor es gelingt, den Kriminellen auszusperren. Und selbst bei einer „Erfolgsquote“ von typischerweise unter einem Promille (weniger als einer von Tausend Empfängern fällt darauf herein) kann es dann schon zu spät sein – im schlimmsten Fall auch schon nach wenigen Sekunden nach Beginn des Angriffs. Oft laufen solche Phishing-Wellen aber tagelang unbemerkt, denn rein formal sind es ja technisch völlig legitime Vorgänge, die auch ein Intrusion-Prevention-System nicht so einfach erkennen kann.

Nutzer muss Teil der Verteidigung werden

Die Sicherheitsverantwortlichen können also heutzutage den Nutzer nicht mehr von den Gefahren abschirmen. In Wahrheit konnten sie das noch nie. Aber es wird exponentiell zunehmen, alleine schon durch die fortschreitende Durchdringung des täglichen Lebens mit „smarten“ Dingen, von Smartphones über Autos bis zur Leuchtstofflampe. Die logische Folgerung ist, dass der Nutzer einer Schwachstelle zu einem Teil der Verteidigung werden muss, ganz genauso wie in der klassischen Arbeitssicherheit beispielsweise. Folgerichtig wird zunehmend am Problembewusstsein der Nutzer gearbeitet, neudeutsch „IT-Sicherheits-Awareness“ genannt. Letztlich geht es schlicht darum, dem Nutzer auf welche Weise auch immer ein paar einfache, aber wesentliche Grundregeln beizubringen.

Es geht dabei um ganz einfache Regeln wie: immer den passwortgeschützten Bildschirmschoner anschalten, wenn man den Platz verlässt, und wenn es nur für ganz kurz ist, sichere Passwörter wählen, Passwörter nicht mehrfach benutzen, wenn nötig Passwort-Safes benutzen, auf der Hut sein vor Phishing, nicht einfach überall draufklicken, nicht jedes Feld in jedem Onlineformular ausfüllen, genau auf die Adresse jeder Webseite achten, bevor man den Link anklickt, eigene Passwörter niemals weitergeben, immer alle Systeme und Programme aktualisieren und Patches einspielen, Backups erstellen und so weiter und so fort.

Natürlich machen sich zahlreiche Experten darüber Gedanken, welche Regeln das sind und wie man sie dem Nutzer

iX-TRACT

- Im Zeitalter der technisch immer komplexeren Sicherheitssysteme und Verteidigungsstrategien führt für Cyberkriminelle der Weg zum Angriffsziel häufig über den Nutzer.
- Auch in früheren Zeiten war Informationssicherheit nie eine Frage der Technik alleine. Allerdings haben sich in den letzten Jahren die Dimensionen vergrößert – insbesondere die der Angriffe.
- Ohne Mithilfe des Nutzers geht es nicht: Verschiedene Ansätze dienen der Sensibilisierung der „Schwachstelle Mensch“. Angenehmer als der Zwang zu Schulungen & Co. ist in jedem Fall eine spielerische und unterhaltsame Herangehensweise. Zwingend erfolgreicher ist sie aber nicht.
- Die Motivation zur Informationssicherheit ist ein immerwährender und häufig auch zäher Prozess: Es engagieren sich in der Regel nur diejenigen Nutzer, die ohnehin schon sensibilisiert sind. Und dennoch darf man nie nachlassen, sich um die anderen zu bemühen.

beibringt. Das Bundesamt für Sicherheit in der Informationstechnik, eigentlich für die Sicherheit der IT des Bundes zuständig, betreibt ein umfangreiches und hochwertiges Webportal unter „BSI für Bürger“ (die Links des Artikels sowie zusätzliche Informationen und Materialien zu Awareness sind zu finden über „Alle Links“ im blauen Kästchen). Das derzeit am häufigsten genutzte Einfallstor für Schadsoftware auf Endgeräten ist das Phishing, meist per E-Mail in Kombination mit gefälschten Webseiten, häufig auch als Spear-Phishing mit gezielt auf einen bestimmten Nutzerkreis (Personalabteilungen, Führungskräfte der Firma XY et cetera) zugeschnittenen Fälschungen.

Wertvolle Informationen zum Schutz dagegen leistet die (im Wesentlichen aus öffentlichen Geldern geförderte) „Forschungsgruppe SECUSO – Security, Usability and Society (Sicherheit, Benutzerfreundlichkeit und Gesellschaft)“ an der TU Darmstadt. Die Palette der öffentlich zugänglichen Ergebnisse geht von einem Onlinetraining für Jedermann über komplette, einfach anzuwendende Trainingsunterlagen für Kurse und Workshops zu dem Thema bis hin zu Browser-Plug-ins, die vor gefährlichen Eingaben im Browser warnen. Sogar einige „Privacy friendly“ Apps für Android stehen zur Verfügung.

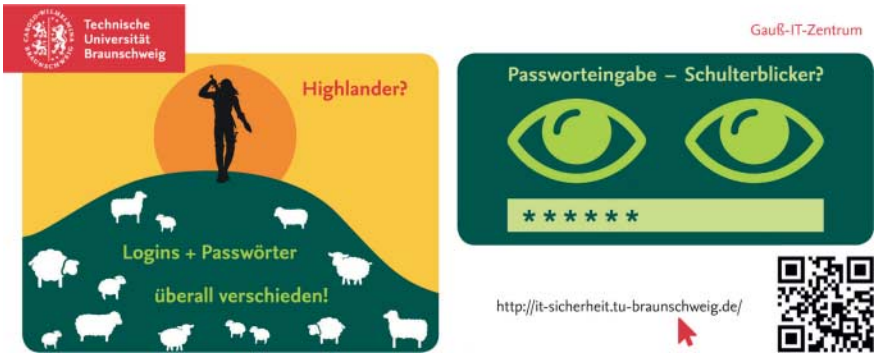
Eine endgültige Lösung gibt es nicht

Es gibt also durchaus „genug“ Informationen im Netz, mit deren Hilfe sich der interessierte Benutzer schlau machen kann. Nur genau da liegt das Problem. Der Nutzer ist selten interessiert. Schließlich sind nicht nur IT-Interessierte gefährdet, sondern alle. Und jeder, der sich Schadsoftware einfängt, gefährdet indirekt oder direkt wieder andere. Es bleibt also nur die Option, gerade die nicht IT-affinen Anwender zu erreichen, auf welchen Wegen auch immer.

Wer sich „in der richtigen“ Welt einmal umsieht, wie man das Problem in anderen Bereichen angeht (zum Beispiel klassischer Arbeitsschutz oder Hygienevorschriften in der Gastronomie), stellt schnell fest, dass das ein Endlos-Job ohne „Lösung“ ist. Vielmehr ist es angeraten, sich an dem Spruch des französischen Autors und Philosophen Albert Camus orientieren: „Wir müssen uns Sisyphos als einen glücklichen Menschen vorstellen.“ Mit anderen Worten, man muss sich mit Situationen abfinden, die man nicht ändern kann. Dem „klassischen“ Problemlösungsdenken in der IT und im Management widerspricht das. Denn hier gilt nicht: Problem –> Lösung –> abarbeiten –> nächstes Problem. Hier ist man immer wieder gezwungen, sich etwas Neues ausdenken, aber man „löst“ das Problem damit nicht.

Wie kann man nun die Aufgabe angehen? Grundsätzlich auf zwei Arten. In der Arbeitswelt klassischerweise durch „Zwang“. Man könnte eine verpflichtende Informationssicherheitsschulung einmal im Jahr abhalten, analog zu oder sogar integriert in die in vielen Bereichen stattfindende Arbeitssicherheitsschulung. Besonders effektiv sind diese Schulungen nicht, genauso wenig wie sie es bei der Arbeitssicherheit sind, aber sie bilden eine Basis.

Schwieriger wird es, wenn man keine Möglichkeiten hat, die Nutzer zu etwas zu verpflichten. An einer Universität beispielsweise kann man die Studenten nicht so einfach zu so etwas „verdonnern“ – und an der Universität, an der der Autor arbeitet, sind das allein schon über 20 000 Personen, zu denen noch einmal um die 5000 Angestellte dazukommen. Eine direkte persönliche Ansprache ist angesichts dieser Zahlen unmöglich. Man versucht also, die Menschen dort abzuholen, wo sie stehen.



Ein Dauerbrenner für jede Awareness-Kampagne ist das Thema Passwort – zu schwach, immer dasselbe, Preisgabe an die Kollegen und weitere Risiken (Abb. 2).

Erstsemester-Einführungen bieten etwa die Möglichkeit, in dem Teil, der über die IT an der Universität informiert, einen kurzen Sicherheitsvortrag unterzubringen. Der IT-Service-Desk als zentraler Anlaufpunkt für Studierende und Mitarbeiter muss regelmäßig auch in Informationssicherheit geschult werden. Die oben genannten Informationsquellen informieren allgemein. Je nach Universität ist es sinnvoll, die Informationen nochmals auf eigene Webseiten zugeschnitten und „lokalisiert“ anzubieten. Auf die eine oder andere Art machen das viele Universitäten. Auch die Allgemeinheit kann meist auf diese Informationen zugreifen.

Sinnvoller Austausch von Informationen und Materialien

Nun muss man aber die Anwender noch dazu bewegen, diese Seiten zu lesen. Dazu muss man immer wieder kreativ werden. Um sich über Ideen auszutauschen und sich gegenseitig Materialien zur Verfügung zu stellen, hat sich für Hochschulen unter dem Dach des ZKI (siehe „Alle Links“) innerhalb des dortigen für Sicherheit zuständigen Arbeitskreises ein formloser Austausch zwischen mehreren „Rechenzentren“ gebildet, an dem sich immer mehr Institutionen beteiligen. So etwas ist natürlich auch auf Branchenverbandsebene in der Wirtschaft sinnvoll.

Aktuelle Beispiele sind etwa die jeweiligen Rechenzentren
– der TU München mit vielen Plakaten, Flyer-Texten und Entwürfen für Tragetaschen (für Erstsemester) sowie umfangreichen Webseiten, über die man sich eine sichere „Passwort-Merkkarte“ erzeugen kann;
– der Hochschule Ansbach mit einer Reihe von über einem Dutzend sehr eingängigen Plakaten (als PDF), die man vielfältig für Aktionen und an Schwarzen Brettern verwenden kann;
– der TU Braunschweig mit umfangreichen Webseiten zur Informationssicherheit, mehreren Vorlesungen als PDF und Videoaufzeichnung sowie Mousepads mit „flotten Sprüchen“ und einem QR-Code plus Link, der zu den Erläuterungen führt. Speziell die Mousepads „gehen weg wie geschnitten Brot“ und werden gerne verwendet. Eine weitere Idee aus der TU Braunschweig sind Schilder (ähnlich den „Bitte nicht stören“-Schildern in Hotels), die man für Aktionen an die Türen hängen kann.

Mehrere Hochschulen bieten auch intern Seminarreihen zum Thema an, sei es für Studenten oder speziell auf die Mitar-

Der *iX*-Awareness-Wettbewerb: Kreativität gefordert!

Es ist egal, ob Sie „Das kann man nebenbei machen"-Administrator in einem Kleinbetrieb, Chief Security Officer eines DAX-Konzerns oder Sicherheitsbeauftragter einer Behörde oder Uni sind – Sie müssen es schaffen, die Aufmerksamkeit der Angestellten für IT-Sicherheit zu schärfen, und zwar dauerhaft. Oder diese Aufmerksamkeit überhaupt erst einmal zu wecken ...

Um diesen Prozess zu unterstützen, hat die Redaktion den *iX*-Awareness-Wettbewerb ins Leben gerufen. Berichten Sie uns, wie Sie die „Awareness" für Sicherheitsprobleme in Ihrer Firma, Behörde oder Bildungseinrichtung verbessert haben! Aber Achtung: Es geht nicht darum, sich einfach irgendetwas auszudenken nach dem Motto „Man müsste mal ...". Es sollte sich bei den geschilderten Ideen um tatsächlich stattgefundene – auch gern noch laufende – Maßnahmen handeln. Und uns interessiert natürlich auch die Resonanz darauf. Wurden Sie auf die Idee angesprochen? Gab es eine spürbare oder wenigstens eine „gefühlte" Änderung des Verhaltens, was den Umgang mit bestimmten Aspekten von IT-Sicherheit angeht?

Die besten drei Ideen werden auf den Internet Security Days 2017 (28./29. September, Phantasialand Brühl) vorgestellt. Die Gewinner sind dazu zum kostenlosen Konferenzbesuch eingeladen. Optimisten sollten also diesen Termin schon einmal blockieren.

Außerdem vergeben wir zahlreiche Sachpreise - eine AVM Fritzbox 7590, einen von den Anti-DDOS-Experten der Firma Myra gestifteten 3D-Drucker und WLAN Access Points von TP-Link. Eine detailierte Beschreibung der Preise ist online zu finden, unter der Webadresse https://heise.de/-3746796 (auch unter „Alle Links" zu finden).

Schildern Sie uns per E-Mail an „post@ix.de" bis zum 31. August 2017, mit welchen Maßnahmen Sie die Awareness steigern konnten. Senden Sie Ihre E-Mail mit der Betreffzeile „Awareness-Kampagne 2017", damit wir sie leichter zuordnen können. Wenn möglich, hängen Sie auch ein Foto oder einen Screenshot zur Illustration Ihrer Awareness-Maßnahme an.

Bitte vergessen Sie nicht, in der E-Mail Ihren vollständigen Namen, den Ihrer Firma oder Behörde einschließlich der Abteilung, wenn es um eine größere Einrichtung geht, sowie Ihre berufliche Funktion zu erwähnen!

Die Gewinner werden in der ersten Septemberwoche benachrichtigt und auf den ISD 2017 vorgestellt. Angestellte der Heise-Mediengruppe sind ebenso ausgeschlossen wie der Rechtsweg.

beiter zugeschnitten. Auch ein Onlinequiz ist eine unterhaltsame Schulungsvariante, das BSI bietet auf seinen „für Bürger"-Seiten eines an.

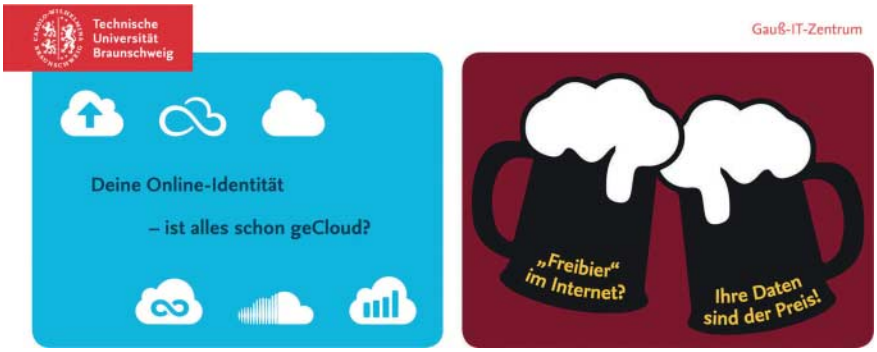
Permanentes Motivieren mit mäßigem Erfolg

Seminare, Vorlesungen, Vorträge, selbst Onlinequiz haben jedoch in der Praxis einen gravierenden Nachteil: Letztlich ist die Beteiligung und das Interesse gemessen an der Größe der Zielgruppe verschwindend gering, und es nehmen oft „die üblichen Verdächtigen" teil, also die Nutzer, die ohnehin schon Eigeninitiative und Interesse zeigen. Diejenigen, die sich nicht um das Thema kümmern und den schlechtesten Wissensstand haben, beteiligen sich an solchen Aktionen nicht. Es hilft also nichts, man muss immer wieder neue Aktionen starten, Plakate aufhängen oder vielleicht auch einmal eine moderne Schnitzeljagd veranstalten (z. B. mit Location-based Services und Kontrollpunkten mit QR-Code).

Und immer wieder sind auch neue Schulungsangebote zu entwickeln, die auf die verschiedenen Zielgruppen zugeschnitten sein müssen – langjährige Verwaltungsangestellte muss man anders ansprechen als junge Studierende Anfang 20. Gerade auf Letztere, auf die sogenannten „Digital Natives", muss man besonders achten. Erfahrungsgemäß gehen sie, geformt von sozialen Medien und unzähligen Apps, besonders sorglos mit ihren Daten und mit IT-/Informationssicherheit allgemein um. Auch das ist eigentlich nichts Unbekanntes in der wirklichen Welt: „Gewöhnung macht unaufmerksam" gilt auch in der „normalen" Gefahrenabwehr. Und wie dort gilt, wo immer es möglich ist, müssen wohl doch verpflichtende Schulungen eingesetzt werden. Rein auf Freiwilligkeit und Interesse zu bauen, wird immer nur einen geringen Teil der Nutzer erreichen.

Sinngemäß gilt das natürlich auch für jegliche Art von Wirtschaftsbetrieben, Behörden oder Organisationen. Ohne Einbeziehen des Nutzers gibt es keine Informationssicherheit. Das bedeutet zusätzliche Arbeit sowohl für die Nutzer als auch für die Zuständigen. Meistens also für „die IT" oder „das Rechenzentrum". Und zwar nicht anstelle der technischen Sicherheitsmaßnahmen, sondern zusätzlich. Dabei war noch nicht einmal davon die Rede, dass in vielen operativen IT-Bereichen/-Abteilungen ebenfalls noch viel „Awareness"-Arbeit zu leisten ist. Viel zu häufig wird immer noch zuerst die Software programmiert oder eingeführt und man definiert Geschäftsprozesse, ganz am Ende soll dann die IT das Ganze schnell und möglichst kostenfrei „sicher machen".

So funktioniert das jedoch nicht. IT-Sicherheit muss man von Anfang an bei jedem Projekt und jeder Programmierung einplanen und „mitdenken". Das betrifft alle IT-Administratoren und Softwareentwickler, nicht nur den Sicherheitsbeauftragten und vielleicht noch den Datenschutzbeauftragten. (ur)



Identitätsschutz im Internet ist wichtiger denn je – ob es um das Vermeiden von Missbrauch der eigenen Identität geht oder um das Preisgeben privater Dinge, die niemanden etwas angehen (Abb. 3).

Christian Böttger

arbeitet als Projektmanager im Stab des Gauß-IT-Zentrums der TU Braunschweig.

Alle Links: www.ix.de/ix1707044