Live-Hacking-Performance als Sensibilisierungsmaßnahme – Ein Erfahrungsbericht

Täglich wird von neuen Gefahren und Bedrohungen in der digitalen Welt berichtet. Finanzielle Schäden, oder auch Rufschädigungen, wie durch die WikiLeaks-Veröffentlichungen steigen täglich. Doch wer ist schuld? Die größte Gefahr für schützenwerte Daten, Unternehmensnetzwerke und den heimischen Computer ist nicht etwa die Technik, sondern das biologische System vor dem Bildschirm. Der Anwender ist mit der Menge an Technologien und digitalen Möglichkeiten überfordert und macht Fehler. Ihm fehlt die Sensibilität für das Thema IT-Sicherheit. Die Firmen, Behörden und Institutionen sind aufgefordert Ihre Mitarbeiter zu schulen, weil eine sichere IT alleine nicht ausreicht. Mit einer Live-Hacking-Performance hat das Institut für Internet-Sicherheit eine Möglichkeit gefunden bei den Anwendern auf unterhaltsame Weise ein Verständnis für das Thema IT-Sicherheit zu erzeugen und dabei spannende Erfahrungen gesammelt.

Die IT ist inzwischen eindeutig die Achillesferse der Unternehmen, Behörden und sonstigen Organisationen. Um die Unternehmen zu schützen werden Sicherheitskonzepte meist für die IT erarbeitet. Aber wird mit Hilfe von IT-Sicherheitsmechanismen allein die notwendige Sicherheit erreicht? Die Frage lässt sich mit einem Blick auf die aktuell größten Gefahren leicht beantworten. Die IT-Sicherheitsstudie von Microsoft und <kes> sagt aus, dass die größte Bedrohung von „Irrtümern und Nachlässigkeiten von Mitarbeitern ausgehen". Malware folgt erst auf dem zweiten Platz. Diese Positionen werden sich in den nächsten Jahren sicher verändern, da die Malwareentwickler alles tun werden, um auf den ersten Platz zu kommen und die Firmen und Behörden alles tun werden, damit die Mitarbeiter weiter hinten in der Liste landen. Leider ist es noch nicht so, dass jede Einrichtung erkannt hat, wie wichtig es ist ihre Mitarbeiter zu schulen. Ein gutes Beispiel ist die Bundesregierung, weil sie die Notwendigkeit erkannt hat.

Es gibt den „Umsetzungsplan Bund" im Rahmen des „Nationalen Plans zum Schutz der Informationsinfrastrukturen". Dieser umfasst verschiedene Kategorien und Maßnahmen und einige davon schreiben vor, dass alle Mitarbeiter aller Behörden in IT-Sicherheit geschult werden müssen.

Jeden Mitarbeiter in Behörden oder auch in Firmen mit dem trockenen Thema IT-Sicherheit zu konfrontieren ist allerdings eine Herausforderung. Erfahrungsgemäß ist eine übliche Frontalpräsentation zum Thema IT-Sicherheit wenig effektiv – vor allem wenn Sie als einzelne Aktion durchgeführt wird. Um Nachhaltigkeit erreichen zu können, müssen zusätzliche Aktionen initiiert werden, die meist zusammengefasst unter dem Begriff Sicherheits-Awareness-Kampagne umgesetzt werden. Eine solche Kampagne sollte nicht nur auf das Arbeitsumfeld abzielen, denn IT-Sicherheit ist auch ein großer Bestandteil des privaten Lebens der meisten Menschen. Wenn ein Mitarbeiter bereits im privaten Kontext ein hohes Sicherheitsbewusstsein an den Tag legt, überträgt er dies auch auf die Arbeit. Es gilt also den Mitarbeiter nicht nur firmenspezifisch, sondern auch grundsätzlich zu schulen. Diese Ausrichtung steigert die Lernkurve enorm, da eine private Betroffenheit jeden einzelnen Anwender noch stärker angeht. Aber wie lässt sich nun dem Mitarbeiter klar machen, dass das Thema IT-Sicherheit enorm wichtig ist, und wie lassen sich die notwendigen Informationen in eine Veranstaltung einbetten?

Die Live-Hacking-Performance

Vor 5 Jahren hat das Institut für Internet-Sicherheit begonnen auf dem CeBit-Messestand live zu zeigen, wie Angriffe ablaufen, um Aufmerksamkeit auf den Messestand zu lenken. Dabei legte das Institut keinen Wert darauf, die neuesten Möglichkeiten von Hackern für Hacker zu zeigen, wie es bereits üblich war, sondern die Inhalte für den „Normal"-Anwender aufzubereiten. Das Feedback auf diese kurzen Demos war so gut, dass damit begonnen wurde diese Live-Hackings als Anwenderschulung anzubieten und umzusetzen.

Das Zielpublikum der Live-Hacking-Performance sind Verwaltungsmitarbeiter ebenso, wie IT-Mitarbeiter oder auch insbesondere die Führungsebene, da diese Sicherheit vorleben sollten.

Die Live-Hacking-Performance wird spielerisch zu zweit in einer Art Rollenspiel durchgeführt. Ein „Hacker" und ein „Anwender" zeigen mit je einem Computer und je eine Anzeigefläche die unterschiedlichen Themenblöcke. Dadurch kann der Anwender alle Vorgänge optimal nachvollziehen. Alle Szenarien orientieren sich an alltäglichen Situationen. Der Vortrag lebt davon, dass alle Gefahren live gezeigt werden. In 90min werden vielleicht max. 8 Folien verwendet. Dadurch ist der Effekt bei den Zuhörern wesentlich höher, als bei „normalen" Vorträgen. Es wird eine positive Betroffenheit für alltägliche Situationen hergestellt – „Flurgespräche" garantiert! Natürlich wird auch jedes Mal erläutert, wie das richtige Verhalten aussieht, um die jeweiligen Angriffe und Situationen zu vermeiden.

Die Erfahrungen

Wir wussten immer dass das größte Problem des Computers das biologische System ist, dass vor dem Computer sitzt und konnten in den Vorträgen erleben, dass dies tatsächlich der Fall ist. Die vielen Reaktionen und Nachfragen der Teilnehmer gaben uns einen Einblick in die Denkweise vieler Anwender und die größten Probleme wurden immer deutlicher. Einige Situationen waren besonders interessant:

Mobilität – Das Führungsebenenproblem

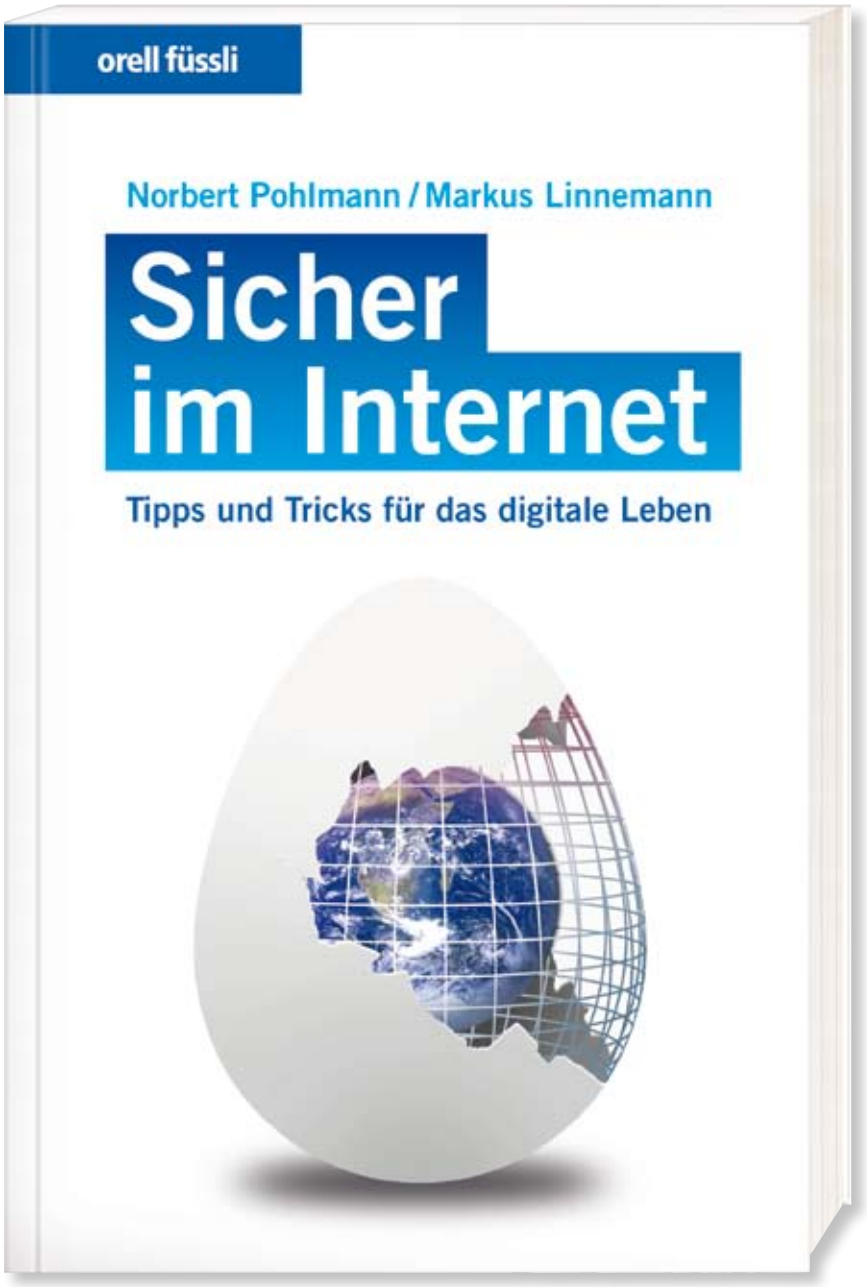
Die Führungsetage bildet gerne eine Ausnahme in Unternehmen, auch wenn es um Schulungen zur IT-Sicherheit geht. Sie sind es, die die Sicherheit vorleben sollten und gleichzeitig die wertvollsten und teilweise geheimsten Informationen verarbeiten.

Die Führungsriege in einem Ministerium sollte einen Ausschnitt des Live-Hackings sehen, damit Sie sich ein Bild schaffen kann, wie ihre Mitarbeiter sensibilisiert werden. Für die Führungsriege ein lästiger Termin, der, ans Ende der monatlichen Besprechung gesetzt, nur stattfindet, weil der Sicherheitsbeauftragte darauf bestand. Nach dem ersten Szenario nach 8min fragten wir, ob Sie obwohl die Zeit um wäre noch weitere Szenarien sehen wollen wür-

den und sofort kam Zustimmung und Sätze wie: „Wir sollten vielleicht auch mal die ganzen 2 Std. mitmachen." Wir sind auf jeden Fall dafür!

Wir waren nicht erstaunt über die Entwicklung, da wir live gezeigt haben, wie quasi jeder, der ein bisschen recherchiert und sich etwas geschickt anstellt in der Lage ist Handys auszulesen, in diesem Fall Smartphones. Mit dem eingesetzten Handytrojaner, der sich übrigens legal erwerben lässt, können Gespräche mitgehört oder SMS und E-Mails gelesen werden. Noch besser ist die Funktion, dass das Handy als Wanze verwendet werden kann – wunderbar um wichtige Geschäftsmeetings abzuhören. Der Anwender kann an seinem Telefon aber nichts erkennen, was auf den Trojaner hinweisen könnte. Klar, dass die Führungskräfte schnell hellhörig wurden, die auf das Telefon angewiesen sind auch gerne dem neusten Trend folgen und moderne Smartphones, wie das iPhone einsetzen.

Diese Trojaner lassen sich zum Beispiel aufspielen, indem der Angreifer das Handy 3-5min in die Hand bekommt. Dies sorgte für viel Aufsehen, als wir zu einer sehr hochkarätig besetzten Veranstaltung in der Mittagspause zum Aufbau kamen und im Vortragsraum sehr viele Handys zum Laden an den Steckdosen fanden – eingeschaltet und ungesperrt. Einige Teilnehmer wurde bei unseren Demonstrationen etwas blass nach der Pause – Lerneffekt hoch!



Mobilität – Viel Handy, wenig Sicherheit(-sbewusstsein)?

Angriffe auf Handys können unterschiedlich initiiert werden, nicht nur mit einem Trojaner, auch zum Beispiel seit Jahren über Bluetooth, speziell bei älteren Handys, weil zum Beispiel Fehler in der Implementierung auf den Handys gemacht wurden. Wir zeigen beispielsweise, wie man alle Telefonnummer so verändert, dass der Hacker bei jedem Anruf mit dem Telefon 3,5 €/min verdient, oder wie man ein Bluetooth Headset abhören kann. Das Feedback zeigt uns, dass es für die Zuhörer schwierig ist Trojaner- und Bluetooth-Angriff auseinander zu halten, obwohl es völlig unterschiedliche Szenarien sind. Das zeigt uns regelmäßig, dass der übliche Anwender mit der Menge an Technologien, die heute in den alltäglichen Geräten verbaut sind überfordert ist. Daher müssen Firmen klare Anweisungen zum Beispiel für die Nutzung eines Firmenhandys vorgeben. Natürlich ist es etwas umständlich bei jeder Nutzung des Smartphones eine PIN einzugeben, aber es ist notwendig. Das Auto schließt man ja auch ab wenn man nur kurz zur Post rein geht.
Überhaupt ist das Handy eine große Sicherheitslücke. Ein Unternehmensnetzwerk wird super geschützt, und alle darin befindlichen Computer mit Schutzmechanismen ausgestattet, aber der Geschäftsführer erledigt alle seine Geschäfte von unterwegs über ein iPAD. Ist dieses Gerät geschützt? Hat es keine Fehler und damit keine Angriffspunkte? Viele Apple-Freunde würden jetzt wahrscheinlich ja sagen, aber das ist natürlich nicht korrekt. Sicherheitslücken sind meist Programmierfehler in der Software und jeder Entwickler macht Fehler. Mobile Geräte können heute zwar fast alles, was ein Computer kann, aber wie viele Kollegen kennen Sie, die ein Anti-Malware-Programm auf dem Handy nutzen? Es gibt einen Grund, warum alle großen Anti-Malware-Hersteller aktuell Produkte für Smartphones auf den Markt bringen, oder es schon getan haben und außerdem befinden sich mobile Geräte nicht dauernd im geschützten Firmennetz.

Privatvermögen als Lernhilfe

Online-Banking am Handy ist für viele bereits Standard ohne drüber nachzudenken, ob das sicher ist. In einem Artikel auf heise-

Online „PIN und TAN auf Reisen", am 22.12.2010 wurden Banking Apps für das iPhone getestet und gravierende Sicherheitsmängel gefunden. mTan, auch SMS-Tan genannt, ist ein sehr sicheres und gutes Online-Banking-Verfahren. Die Sicherheit resultiert vor allem aus der Nutzung unterschiedlicher Kanäle, sprich Computer und Handy. Natürlich egalisiert sich dieser Vorteil, wenn jenes Smartphone zum Online-Banking verwendet wird, das auch die SMS mit der TAN empfängt. Überhaupt ist online-Banking ein beliebtes Ziel für Angreifer, wie Phishing und Pharming-Attacken immer wieder beweisen. In der Live-Hacking-Performance werden beide Szenarien gezeigt. Beim Pharming lockt der Hacker den Anwender auf eine gefälschte Bankseite, obwohl der die Web-Adresse der Bank mit der Hand eingibt und auch eine SSL-Verschlüsselung vorliegt. Das Zertifikat ist allerdings gefälscht. Einer unserer Tipps, um den Schwindel zu bemerken ist es den Fingerabdruck des Zertifikats der Webseite anzeigen zu lassen, den Bankberater anzurufen und den Fingerabdruck mit ihm abzugleichen. Probieren Sie es aus, die wenigsten Bankberater wissen etwas mit dem Fingerabdruck anzufangen – Ja, wir machen auch Schulungen für Banken!

Szenarien zum Online-Banking betreffen jeden auch privat und sind somit ideal geeignet, damit jeder merkt, dass ihn das Thema IT-Sicherheit etwas angeht, denn hier geht es um das eigene Ersparte. So kann leicht ein Bewusstsein für diese Zusammenhänge bei den Mitarbeitern geschaffen werden. Diese Art private Vorgänge sicherheitskritisch zu betrachten überträgt sich auf das Verhalten der Mitarbeiter im Unternehmen.

Das Passwort-Dilemma

Ein ewiger Klassiker in diesem Kontext ist das Thema „Passwörter". In über 50% aller Fälle sind wir in Organisationen zum Vortrag deren Passwortregeln Passwörter mit 6 Stellen ohne Sonderzeichen und Co. zulassen und wo es Gang und Gebe ist Passwörter weiterzugeben. Entscheidend für Nachlässigkeiten mit Passwörtern ist häufig das „Stresslevel" der Personen. In einem Fall haben wir mit unserem Vortrag begonnen, indem wir von allen Teilnehmern die E-Mail-Adresse und das zugehörige Passwort haben wollten. Natürlich haben die Teilnehmer sehr zurückhaltend reagiert und uns nicht mal ihre Namen geben wollen (übrigens trotz Namensschilder), weil Sie ja wussten, warum wir da waren. Eine Person kam 10min zu spät. Wir haben sie direkt angesprochen und begrüßt und erklärt, dass sich bereits alle eingetragen hätten und wir auch von diesem Teilnehmer noch Mail-Adresse und Passwort benötigen. Der Teilnehmer hatte ein schlechtes Gewissen, stand plötzlich im Mittelpunkt und hat daher sofort Auskunft gegeben. Zum Glück konnten wir das stoppen bevor ein Passwort ausgesprochen war. Die Wichtigkeit von Passwörtern ist offensichtlich noch nicht jedem bewusst. Hätten wir nach dem Hausschlüssel gefragt, hätten wir ihn sicher nicht erhalten.
In der Live-Hacking-Performance zeigen wir, wie schnell ein heutiger Grafikkarten-Computer sechsstellige Hashwerte von Passwörtern knacken kann. Ein Teilnehmer rief uns zu, dass sein Passwort sicher wäre und wir es nicht knacken könnten und wir sollten es doch ausprobieren. Um sein Passwort knacken zu können musste er es uns erst nennen, damit wir einen Hash bilden können. Er gab es uns! Wir könnten es nicht glauben.

Ein Teilnehmer kam nach einer Live-Hacking-Performance zu uns und sagte: „Guter und ich habe die Probleme mit dem Passwort auch verstanden, aber Sie meinen das nicht ernst, stimmt´s, also nehme ich weiter mein 6stelliges Passwort für alle Dienste ...". Da war uns klar, allen können wir nicht helfen!

Social Engineering – Die Basis aller Angriffe

Die vorigen Fälle zeigen die vielleicht größte Gefahr: das „Social Engineering". Es ist unheimlich einfach mit dem richtigen Vorwand an Informationen oder in Gebäude zu kommen. Wir haben mehrfach auf Gängen von Unternehmen Mitarbeiter gefragt, wie sich die Benutzernamen im Unternehmen beim Einloggen zusammensetzen und erhielten eigentlich immer direkt Antwort, auch direkt in den Vorträgen. Meist setzen sich die Benutzernamen aus Teilen des Vor- und Nachnamens zusammen, z. Bsp. „Vorname.Nachname". Damit haben wir schon in Kombination mit einer Telefonliste, die oft in öffentlich zugänglichen Räumen in Unternehmen ausliegen einen Teil der Zugangsdaten zum Intranet. Dann muss man sich noch die Passwörter organisieren oder mit dem Telefonverzeichnis in dem auch die Mailadressen stehen trojanisierte Mails an alle Mitarbeiter verschicken. Aber der erste Schritt ist getan, ganz ohne technische Hilfe. In der Live-Hacking-Performance werden solche Angriffe ausprobiert und aufgezeigt, wie leicht es ist an Informationen zu kommen und welche Informationen schützenswert sind. Social Engineering findet aber nicht nur Face-to-Face statt, sondern auch übers Telefon oder über das Internet.

Soziale Netzwerke als Angriffsplattform

Soziale Netzwerke erfreuen sich großer Beliebtheit. Daher ist es viel leichter Malware und Links auf infizierte Web-Seiten in sozialen Netzwerken zu verbreiten, als extra direkte Mails zu verschicken. Auch Phishing-Attacken, Mobbing und andere Angriffe sind inzwischen Teil der Online-Communitys. Neben der traurigen Tatsache, dass die Anwender heute ganz von alleine massenhaft schützenswerte Informationen in den Netzwerken verbreiten. Gerne werden Firmentechnologien in Technikerforen diskutiert, wodurch Firmengeheimnisse preisgegeben werden. Im privaten Sektor gibt es eine Studie, dass in Amerika über 50% aller Befragten mehr Informationen ihrem Facebook-Account anvertrauen, als ihren besten Freunden. Auch ein klarer Fall von mangelndem Verständnis. Hier ist also auch wieder der Anwender das Problem, neben den Sicherheitsrisiken, die von den Betreibern eingebaut werden. Beispielsweise fand ein Kollege im Institut einen Fehler bei Facebook. Es wurden Zugangsdaten inklusive Passwort nicht verschlüsselt, sondern nur Base64-codiert versendet, dabei sagen die AGBs, dass alle sicherheitskritischen Daten verschlüsselt versandt werden. Der Fehler wurde nachdem das Problem bei „Monitor" gezeigt wurde, von Facebook behoben und zeigt den Zuhörern bei der Live-Hacking-Performance plakativ wo die Fehlerteufel stecken können.

Malware – Die zweitgrößte Gefahr

Neben dem biologischen System vom dem Computer ist die Malware laut der Microsoft-Sicherheitsstudie das größte Problem. Deshalb beginnt unsere Demo bei den Vorträgen mit einem Trojanerangriff des „Hackers" auf den „normalen Anwender". Der normale Anwender erhält eine Mail von Bernd, wie er denkt sein ehemaliger Schulkamerad, oder der Tenniskumpel, aber die Mail ist vom Hacker, denn Absender

von Mails lassen sich fälschen. In der Mail ist ein Link auf eine infizierte Webseite oder ein infiziertes PDF im Anhang, wodurch der Trojaner-Angriff gestartet wird.

Bei dem Szenario wird absichtlich ein Windows verwendet, dass ein paar Wochen nicht gepacht wurde und keine, außer die von dem jeweils gezeigten Windows (Win7 oder XP) bereits mitinstallierten, Anti-Malware Tools installiert hat. Studien belegen dass weltweit weniger als 3% aller Systeme vollständig auf dem aktuellen Stand sind. Aktuell ist ein System erst, wenn auch die Zusatzsoftware, wie PDF und Co aktuell gehalten wird. Es gibt Angriffe gegen die ein Anwender machtlos ist, aber gegen die üblichen Angriffe ist er mit einem aktuellen System, gutem Anti-Malware-Programm und gesundem Menschenverstand geschützt. In der Demo wird entsprechend auch gezeigt, dass der Angriff unter diesen Voraussetzungen nicht mehr funktioniert und warum es so einfach ist nicht aktuelle Systeme anzugreifen.

Die Betriebssystem-Gretchenfrage

Die Standardfrage, die nahezu immer gestellt wird ist, ob denn Mac und Linux sicherer seien, als Windows. Wir erläutern dann, dass vom Betriebssystemaufbau her im Grunde alle gleich unsicher sind, aber Windows am häufigsten angegriffen wird, weil es die meisten Anwender nutzen. Mac-User, die sich bisher in Sicherheit wähnten müssen aber langsam vorsichtig werden, da die Marktanteile steigen. In den USA hat Apple als Hersteller die 10% Marktanteilgrenze überschritten (Gartner) und in der Schweiz nutzen ca. 20% Mac-Betriebssysteme (AT Internet). So langsam wird es lukrativ Mac anzugreifen. Schon 2008 wurde ein MacBook über den Browser Safari auf dem Hacker Wettbewerb PWN 2 OWN als erstes in unter 2min gehackt. Letztes Jahr im selben Wettbewerb sah das Ergebnis ebenso aus, auch für das iPhone. Natürlich erging es den Konkurrenten nicht viel besser. Aber es wird klar, dass sich auch der Mac-User schützen muss.

In diesem Kontext wird auch immer gefragt, welches Anti-Malware-Programm denn am besten wäre und ob Gratis Virenscanner ausreichen würden. Da wir erfahren mussten, dass sich doch wenige wirklich mit Ihrem Computer auskennen und in der Lage wären, die verschiedenen notwendigen Gratis-Tools ordentlich zu konfigurieren, empfehlen wir Kaufsoftware der bekannten Hersteller als Komplettpaket einzusetzen. Auch hier helfen die Live-Hackings das Verständnis zu schaffen, das 35 Euro im Jahr nicht zu viel Geld für die Sicherheit der eigenen Daten ist.

Erkenntnisse aus den Live-Hacking-Awareness-Vorträgen

Eine spannende Erkenntnis für uns war es, dass die jeweilig behandelten Themen für völlig unterschiedliche Gruppen von Anwendern nahezu gleich waren. Egal ob wir Mitarbeiter aus der IT-Abteilung, Manager, Präsidenten, Büroangestellte oder Polizisten geschult haben, die Themen, Fragen und die Bedrohungen sind für fast alle gleich. Unterscheidungen gab es eher in der Tiefe in der die Szenarien erläutert wurden. Es zeigt, dass für eine Sensibilisierung keine Spezialfälle behandelt werden müssen, sondern ein grundlegendes Verständnis vermittelt werden sollte.

Die Live-Hacking-Performance schafft es durch einfache plakative Darstellungen von alltäglichen Szenarien positive Betroffenheit herzustellen. Damit eignet sich die Live-Hacking-Performance sehr gut als Kick-Off für eine Awareness-Kampagne zum Thema IT-Sicherheit, denn der Vortrag alleine reicht nicht. Es müssen Aktionen folgen um eine Nachhaltigkeit zu erreichen. Das Thema IT-Sicherheit ist nicht trocken, und kann für fast jeden Anwender interessant dargestellt werden.

Unterhaltsamkeit ist ein besonders wichtiger Aspekt, um die Anwender für das Thema zu begeistern. So wird auch die Aufmerksamkeit derer erreicht, die technisch nicht so affin sind. Wichtig ist es für alle gezeigten Szenarien auch die Lösung an die Hand zu geben, da es nichts bringt jemanden Angst zu machen und dann im Regen stehen zu lassen.

Wir haben auch ein Buch mit dem Titel „Sicher im Internet – Tipps und Tricks für das digitale Leben" zu dem Thema geschrieben, um dem Anwender auch in dieser Form Informationen an die Hand zu geben, gemäß dem Live-Hacking-Rezept: Einfach verständlich, mit vielen Hilfen und unterhaltsam.

Die meisten Anwender glauben, dass Sicherheit den (Arbeits-)Alltag stark einschränkt, bzw. viele lästige zusätzliche Aufgaben beinhaltet. Es stimmt das einige Aktionen hinzukommen, aber diese sind ungefähr so aufwendig, wie beim Autofahren den Gurt anzulegen. Darum wird zurzeit ein Folgevortrag entwickelt, der erneut live im Rollenspiel zeigt, wie ein sicherer Alltag mit Mailverschlüsselung, Festplattenverschlüsselung, Backup und Co aussieht.

Unsere Erfahrungen haben gezeigt, dass die Sensibilität von Anwendern im sicheren Umgang mit der IT bisher eher gering ist. Es ist notwendig, dass die Organisationen Ihre Mitarbeiter schulen, für die private Sicherheit, aber vor allem um Organisationsdaten und Geheimnisse zu schützen.

Wir würden uns freuen wenn wir in Zukunft die Frage nicht mehr beantworten müssten, ob es ungünstig wäre im Internet-Café im Urlaub seine Online-Bankgeschäfte zu tätigen. Und wenn Manager Ihre sicherheitskritisch eingestuften Dokumente nicht neben uns im Zug auf ihrem iPhone oder Notebook lesen und wir sie daher mitlesen müssen. ■

Prof. Dr. Norbert Pohlmann, Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen

Markus Linnemann, Geschäftsführer des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

Weitere Artikel/News zum Schwerpunkt unter www.datakontext.com/mobile