3/2016

ELEmente

Das Magazin für Business-Kunden der Emscher Lippe Energie

TOP EVENT

Erleben Sie Hacking live vor Ort

SEITE 4

So schützen Sie sich und Ihr Unternehmen vor Cyberkriminellen

HILFE EIN VIRUS!

IT-Experte Professor Norbert Pohlmann

INNOVATIV

Aramark bietet individuelle Catering-Konzepte

BLENDEND

Unternehmen profitieren von LED-Lösungen der ELE

Diagnose: Unsicher

Ob auf dem Smartphone oder im Firmennetzwerk: Überall lauern Gefahren von Viren, Trojanern und Cybergangstern. Professor Nobert Pohlmann, Direktor des Instituts für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen, über die Möglichkeiten, sich zu schützen.

Herr Pohlmann, bei Ihren Vorträgen zur IT-Sicherheit hacken Sie sich gern mal in die Smartphones Ihrer Zuhörer. Ist das wirklich so einfach?

Tatsächlich haben wir Zuhörern schon Sicherheitslücken von Smartphones vor Augen geführt, und zwar mit einfachsten Mitteln. Wir haben lediglich das ausgenutzt, was die Geräte von sich aus preisgeben. Wenn ein Smartphone zum Beispiel eine drahtlose Internetverbindung, ein WLAN, sucht, wird eine Liste mit den bisher genutzten WLANs sichtbar. Allein hieraus lassen sich sensible Informationen ziehen wie die Aufenthaltsorte der Nutzer, zum Beispiel ein Nachtklub. Der Aha-Effekt ist dann schon groß. Das ist allerdings kein wirkliches Hacking, dazu ist dann doch etwas mehr notwendig. Auch das beherrschen wir: Mit Live-Hacking-Events spiegeln wir Sicherheitsprobleme in Unternehmen.

Unter ausgefeilten Cyberangriffen scheinen vor allem große Firmen zu leiden. Wie sieht die Bedrohungslage für kleine und mittelständische Unternehmen aus?

Trotz Innovationen wie Verschlüsselungstechniken oder Firewalls habe ich es in meiner über 30-jährigen Berufslaufbahn noch nicht erlebt, dass sich die Risiken irgendwann mal verringert hätten. Konzerne verfügen heute über spezielle Abteilungen für die IT-Sicherheit mit Dutzenden von Mitarbeitern, trotzdem wissen sie nicht immer, wie sie sich vor bestimmten Cybergefahren schützen sollen. Kleinere Firmen haben oft nicht einmal einen IT-Beauftragten.

Und hinken beim Thema IT-Sicherheit gefährlich hinterher?

Kleinen und mittelständischen Unternehmen wird ständig vorgeworfen, nicht genug für die IT-Sicherheit zu tun. Auf der einen Seite stimmt das natürlich. Typisch für einen Mittelständler ist eine Webseite, die aus Kostengründen unprofessionell programmiert ist, denn sie soll nur eine digitale Visitenkarte sein. Das Problem ist, dass so eine Webseite leicht von Hackern gekapert werden kann, um Malware wie Viren und Trojaner zu verbreiten. Ein weiterer Punkt sind Sicherheitslücken in den IT-Systemen selbst, ebenfalls ein Risiko sind unbedarfte Mitarbeiter, und natürlich ist auch der Mittelstand das Ziel digitaler Wirtschaftsspionage. Auf der anderen Seite jedoch können kleinere Unternehmen gar nicht so viel schulen und absichern, wie es Risiken gibt.

Das würde wohl sehr teuer kommen.

Als Experte für Cybersicherheit checkt Prof. Norbert Pohlmann digitale Systeme auf mögliche „Schädlinge".

Die Kosten sind ein wichtiger Punkt. Entscheidend aber ist, dass die Firmen sich überfordert fühlen. Sie wissen schlicht nicht, wo sie ansetzen sollen.

Was wäre Ihrer Meinung nach ein geeigneter Ansatz, um sich ausreichend zu schützen?

Es gibt eine Faustregel, nach der fünf Prozent der Daten so wichtig sind, dass ohne sie das Überleben der Unternehmung gefährdet ist. Bei Dienstleistern können das Kundendaten sein, bei produzierenden Firmen Entwicklungsdaten. Unternehmen sollten diese fünf Prozent identifizieren und darauf fokussieren, die entsprechenden Systeme besonders sicher zu machen. Auf diese Weise ist die Komplexität enorm reduziert. Wenn dann noch Programme zum Schutz vor Schadsoftware, eine Datenverschlüsselung, ein Backup-System sowie eine Firewall zum Einsatz kommen, die Mitarbeiter geschult werden und die Systeme regelmäßige Updates erhalten, sind Firmen schon ziemlich gut gewappnet.

Dass wir uns aber irgendwann ganz entspannt zurücklehnen können, bleibt wohl ein Wunschtraum.

Wir leben leider mit Technologien, die per se unsicher sind. Wenn Sie mich nach einer Vision für die Zukunft fragen, muss es meiner Auffassung nach zu einer Produkthaftung der IT-Hersteller kommen.

Sie meinen, wenn meine Software für Viren angreifbar ist, dann könnte ich den Hersteller in die Pflicht nehmen?

ERLEBEN SIE DIE TRICKS DER HACKER LIVE!

Top Event

Freuen Sie sich auf eine außergewöhnliche Veranstaltung in einer außergewöhnlichen Location: ein Live-Hacking-Event mit Professor Norbert Pohlmann, exklusiv für Leser der ELEmente. Der IT-Experte wird Ihnen demonstrieren, wie Cyberkriminelle arbeiten, wie leicht viele Unternehmen und Anwender es ihnen machen, auf sensible Daten zuzugreifen und wie Sie sich wirkungsvoll vor Hackern schützen können. Es wird in jeder Hinsicht ein Abend mit neuen Perspektiven: Wir laden Sie ein ins Videokunstzentrum im Gelsenkirchener Nordsternturm (Bild). Hier genießen Sie aus 80 Metern Höhe eine beeindruckende Aussicht über das Ruhrgebiet.

Datum: 29. September 2016, 17.30 bis 19.30 Uhr
Ort: Videokunstzentrum im Nordsternturm

Melden Sie sich am besten gleich zu dieser besonderen Veranstaltung an – die Zahl der Plätze ist begrenzt, Anmeldungen werden nach Datum des Eingangs berücksichtigt. Die Teilnahme ist für die Leser der ELEmente kostenlos.

Bitte informieren Sie uns bis zum 15. September 2016, ob Sie dabei sind und ob Sie eine Begleitperson mitbringen. Einfach eine E-Mail schreiben: **uta.radeler@ele.de**

Noch ist die Zeit nicht reif dafür, aber genau das muss kommen. Um es auf den Punkt zu bringen: Mit Software ist es im Moment so, als würde ein Autohersteller ein Fahrzeug ohne Bremsen verkaufen und dem Kunden sagen, er muss für die nötige Sicherheit selbst sorgen. Das wird sich in Zukunft ändern müssen. Ein anderer Teil der Zukunft besteht darin, Informationstechnik nicht mehr selbst zu besitzen, sondern sie über das Cloud-Computing lediglich zu nutzen. Gerade für den Mittelstand ist das interessant, denn die Verantwortung für die IT-Sicherheit übernehmen die Anbieter.

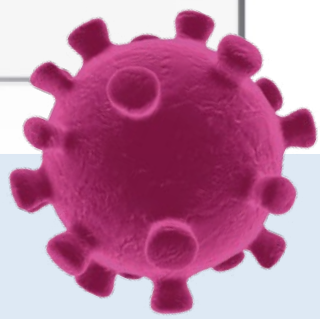
Beim Thema Cloud-Computing haben viele Unternehmen allerdings noch große Vorbehalte.

Es ist wichtig, auf einen vertrauenswürdigen Dienstleister zu setzen. Die Alternative ist, dass sich jede Firma einen IT-Sicherheitsbeauftragten zulegt. Das halte ich allerdings in vielen Fällen nicht für besonders realistisch …

Wie schützt die ELE ihre Daten?

„Der Schutz vor Cyberkriminalität hat für uns bei der ELE eine sehr hohe Priorität, weil wir ja Daten von vielen Tausend Kunden in unseren Systemen pflegen. Technisch schützen wir uns natürlich mit laufend aktualisierten Firewall-Systemen und Virenscannern. Auch unsere Netzleitwarte wird gerade mit einem hochmodernen Netzleitsystem ausgestattet, das höchsten aktuellen Sicherheitsstandards entspricht. Neben solchen technischen Aspekten ist auch der Umgang unserer Mitarbeiter mit dem Thema Datensicherheit extrem wichtig. Alle haben sich auf eine strenge „Security Policy" verpflichtet und werden in Schulungen immer wieder auf den neuesten Stand gebracht. Mit einem aufwendigen Berechtigungssystem stellen wir zudem sicher, dass nur jene Mitarbeiter Zugang zu Kundendaten bekommen, die auch damit arbeiten müssen."

Rolf Borgmann,
Leiter Informationsmanagement
bei der ELE



Wo lauern die Risiken?

Das Institut für Internet-Sicherheit hat zentrale Schwachstellen identifiziert:

MOBILE GERÄTE

Die Vorteile von Smartphones und Tablets im Geschäftsbereich sind bestechend. Doch sind die Angriffsflächen groß, zumal Mitarbeiter die Geräte oft nicht nur beruflich, sondern auch privat und damit abseits von den Sicherheitsmechanismen des Unternehmens nutzen. Der Ausweg: Detaillierte Regelungen dazu, welches Gerät in welchem Zusammenhang genutzt werden und auf welche Daten zugreifen darf.

FEHLERHAFTE SOFTWARE

Hochwertige Software weist pro 1.000 Zeilen Programmcode im Schnitt 0,3 Fehler auf. Gängige Betriebssysteme bestehen aus rund 10 Millionen Codezeilen, die Zahl der Fehler summiert sich so auf 3.000. Fehler, die sicherheitsrelevant sein können. Experten fordern, dass die Softwarehersteller ähnlich wie die Autoindustrie eine Produktverantwortung übernehmen – wenn ein Auto fehlerhaft ist, wird es zurückgerufen und nachgebessert.

ZU WENIG SCHUTZ VOR MALWARE

Viren, die PCs lahmlegen, oder Trojaner, die Daten ausspähen – jeder 15. Rechner ist nach Schätzungen des Instituts für Internet-Sicherheit von digitalen Schädlingen („Malware") befallen. Nicht immer können Antivirenprogramme sie erkennen, und wenn, dann können sie den Schaden lediglich begrenzen. Besser sind neue, proaktive Sicherheitssysteme, die einen Virenbefall erst gar nicht zulassen. Sie sind gänzlich anders aufgebaut als die bislang üblichen Lösungen.

UNSICHERE AUTHENTIFIKATION

Selbst sensible Daten sind lediglich mit einem Passwort geschützt. Um sich die Passwörter besser merken zu können, vergeben viele Anwender unsichere Passwörter – oder nutzen gute mehrfach. Weit sicherer ist eine zusätzliche Authentifizierung etwa mit dem Sicherheitschip im neuen Personalausweis. Er kann – ein entsprechendes Lesegerät vorausgesetzt – als sicherer Schlüssel dienen.

UNSICHERE WEBSEITEN

Malware verbreitet sich hauptsächlich über laienhaft programmierte Webseiten. Hacker können sie leicht kapern, denn oft wird nur auf Layout und Inhalt von Webseiten geachtet, das Thema IT-Sicherheit spielt keine Rolle. Mit einer professionell programmierten Webseite schützen Unternehmen sich und ihre Kunden.

WIRTSCHAFTSSPIONAGE

Einer Erhebung des Vereins Deutscher Ingenieure (VDI) zufolge gehen der deutschen Wirtschaft jährlich 100 Milliarden Euro durch Plagiate und Patentrechtsverletzungen sowie den Ausfall von IT-Systemen und Fertigungsstätten nach Cyberattacken verloren. Gemeinsam mit den IT-Herstellern müssen neue Sicherheitskonzepte und -techniken entwickelt und bereits verfügbare auf breiter Basis eingesetzt werden, zum Beispiel Verschlüsselungslösungen oder Sicherheitsbetriebssysteme mit Isolierungstechnologien.