

Gesunder Menschenverstand – ein Sicherheitsaspekt

Meist herrscht im IT-Alltag Sorglosigkeit. Dies freut Hacker, Virenschreiber und Phishing-Fallensteller. Dabei wäre mit gesundem Menschenverstand schon viel erreicht und mit einem Awareness-Programm zumindest der erste Schritt getan. *Carlos Rieder*



Carlos Rieder
Prof. Dipl. El.-Ing. FH, ist Leiter des Competence Center IT-Security an der Hochschule für Wirtschaft Luzern sowie Partner isec ag, Security-Consulting, Luzern

Den PIN-Code des Bancomaten weitergeben? Sicher nicht! Das Passwort für mein Benutzerkonto meiner Stellvertretung geben? Warum nicht, schliesslich muss er während meiner Abwesenheit arbeiten können. Unser Bewusstsein im Umgang mit IT ist noch nicht genügend geschärft. Es fehlt oft an einfachsten Verhaltensregeln. Blindes Vertrauen in die Technik, Gleichgültigkeit und Sorglosigkeit bergen grosse Risiken. Aber auch die Meinung, der Hersteller werde schon für die Sicherheit gesorgt haben, ist fahrlässig. Über Jahre

wurde geklagt, dass der Umgang mit Computern zu kompliziert sei. Automatismen sollten komplexe Aufgaben, wie zum Beispiel das automatische Öffnen von Mails, erledigen. Damit wurde dem Benutzer der Einsatz der IT so einfach wie möglich gemacht. Mit diesen «benutzerfreundlichen» Automatismen wurden jedoch viele Schwachstellen eingebaut, welche von Hackern gerne ausgenutzt werden.

Vorfälle der jüngsten Vergangenheit zeigen, dass mit technischen Massnahmen allein nicht alle Gefahren der IT-Sicherheit gebannt werden können. Beispielsweise wird beim Phishing der Benutzer plump getäuscht und alle – eigentlich sehr wirkungsvollen – Sicherheitsmechanismen werden ausgehebelt. Dies verdeutlicht, dass ein entscheidender Teil der Sicherheit auf dem individuellen Verhalten basiert. Durch gezielte Förderung der Awareness soll das Verhalten sicherer werden und damit das Potenzial jedes Einzelnen zur Abwehr von Angriffen genutzt werden.

Umgang mit IT-Risiken gehört zur Allgemeinbildung

Um mit den Risiken richtig umgehen zu können, muss man sich ihrer bewusst werden. Hier sind Aufklärung und Ausbildung gefragt,

und zwar im breiten Stil. Gezielte, auf das Publikum zugeschnittene Ausbildungskonzepte sind Voraussetzung, um die nötige Kompetenz aufzubauen. Aufgrund der grossen Verbreitung der IT, im Beruf wie auch zu Hause, gehört dieses Wissen zur Allgemeinbildung. Die IT ist aus unserer Welt nicht mehr wegzudenken. Das Wissen über den sicheren Umgang mit IT ist ebenso wichtig, wie die Namen

der Gebirge in Europa zu kennen, und muss deshalb in der Grundausbildung vermittelt werden.

Das Schwerk

wicht muss auf ein gesundes Misstrauen gelegt werden: Nicht alles, was der Computer sagt, ist «wahr». Ohne zu hinterfragen wird «OK» geklickt – nach dem Grundsatz «Es wird ja schon nichts passieren». Richtig, es besteht kaum Gefahr, dass einem der Arm abgerissen wird. Die Risiken liegen aber zum Beispiel im Datenverlust. Dies verursacht im ersten Moment zwar keine Schmerzen, die Folgen können aber verheerend sein.

Blindes Vertrauen in die IT birgt Risiken. Etwas mehr Skepsis – gesunder Menschenverstand (GMV) eben – zahlt sich aus. Sich zuerst zu fragen «Macht diese Mitteilung in diesem Zusammenhang Sinn?» wäre eine gute Taktik. Wie beim Rechnen spricht man von einer Überschlagsrechnung und erkennt schnell, dass 15x3 nicht 450 geben kann. Vielen Benutzenden fehlt eine solche Kontrollmechanik. Wie sonst können vertrauliche Informationen an völlig Unbekannte weitergegeben werden?

Den gesunden Menschverstand durch ein Awareness-Programm schärfen

Der GMV muss im Bereich der IT geschärft werden. Nur so können aktuelle und zukünftige Angriffe auf die IT – und insbesondere die

«Unser Bewusstsein im Umgang mit IT ist noch nicht genügend geschärft.»

Wissen alleine genügt nicht, das korrekte Verhalten ist entscheidend

Daten verhindert werden. Die Schärfung des GMV geschieht durch Aufklärung und Schulung im Rahmen eines Awareness-Programms. Folgende Attribute charakterisieren ein erfolgreiches Awareness-Prgramm:

• **Prägnant**

Besser drei Themen intensiv erläutern als zehn im Schnellverfahren. Die Themenpalette ist enorm gross, aber das Verhalten soll geändert werden. Wissen alleine genügt nicht, Umdenken ist nötig. Die Erfahrung zeigt beispielsweise, dass viele Benutzer eigentlich wüssten, wie ein starkes Passwort aufgebaut sein muss. Dennoch werden aus Bequemlichkeit und Unverständnis bezüglich der Auswirkungen schwache, einfacher zu merkende Passwörter eingesetzt. Einige wenige Themen schwer gewichtig zu behandeln und auch

durchzusetzen bringt mehr, als über alle Vorschriften pauschal zu dozieren. Die Auszubildenden «hängen» mental ab und haben am Schluss gar nichts mitbekommen. Praktische Umsetzungen bewirken mehr als grosse Theorien. Mit Beispielen aus einem ähnlichen Umfeld kann man Konsequenzen aufzeigen und so das geforderte Verhalten begründen.

• **Abgestimmt**

Um die Benutzer nicht zu überfordern und auch nicht zu unterfordern, sollte die Ausbildung zielgruppenorientiert erfolgen. Gerade das oberste Management muss unbedingt stufengerecht aufgeklärt werden. Denn nur mit der «Rückendeckung» durch das Management ist der langfristige Erfolg garantiert.

Auch die IT-Mitarbeitenden müssen individuell ausgebildet werden. Trotz Fachwis-

sen kommt aufgrund des Drucks im operativen Geschäft die IT-Sicherheit oft spät zur Diskussion. Bei dieser Gruppe muss das Verständnis zwingend gefördert werden, zumal das Schadenspotenzial besonders gross ist. Eine interessante Gruppe sind die Auszubildenden. Sie verfügen vielfach über grosses Interesse an der IT und über mehr Zeit als andere Mitarbeiter. Die Auszubildenden könnten zu «Missionaren der IT-Sicherheit» geschult werden und so das Wissen in die Abteilungen der Unternehmen hinaustragen.

• **Stetig**

Steter Tropfen höhlt den Stein! Regelmässige Wiederholungen führen zum Erfolg.

Der Mensch vergisst gerne, besonders wenn etwas zusätzlichen Aufwand bedeutet. Ehemals klar vereinbarte und institutionalisierte

Vorgänge gehen klammheimlich unter. Die IT-Sicherheit muss immer wieder sichtbar gemacht werden. Nur so kann der einmal erreichte Level gehalten werden.

Auf drei Schauplätzen sollte das Awareness-Programm greifen:

• **Ausbildung**

Ein Grundpaket von Wissen muss durch Ausbildung vermittelt werden. Neben dem Aufbau von Kompetenz muss auch eine Änderung des Verhaltens erreicht werden. Dazu eignen sich klassische Unterrichtsformen oder auch Mischformen mit neuen Ausbildungsmethoden wie z.B. Computer- oder Web-based Training (CBT). Reines Selbststudium, basierend auf Büchern oder unterstützt durch CBT, fördert tendenziell nur das Wissen, ohne das Verhalten zu verändern.

Der persönliche Kontakt mit dem Sicherheitsbeauftragten in der Ausbildung ist sehr wertvoll. Die Sicherheit bekommt ein Gesicht und ist nicht nur Papier. Ausserdem hat der Sicherheitsbeauftragte die Möglichkeit, die Probleme der Basis zu erkennen.

• **Flankierende Massnahmen**

Das Thema Security sollte immer präsent sein, zumindest im Hintergrund. Regelmässige Beiträge im Unternehmens-Newsletter, Umfragen oder Erfolgsmeldungen per E-Mail und auch Kontrollen lassen das Thema bei den Mitarbeitenden immer wieder in den Vordergrund rücken. Die Grundlagen der IT-Sicherheit des Unternehmens, auf welchen auch die Ausbildung aufbaut, müssen für alle einfach abrufbar sein. Idealerweise wird hier das Intranet eingesetzt. Ein prominenter und aktueller Auftritt fördert die IT-Sicherheit nachhaltig.

• **Kampagnen**

Um das Thema der IT-Sicherheit immer wieder ins Zentrum zu rücken, sind Kampagnen durchzuführen. Diese sollen die Aufmerksamkeit der Benutzenden auf sich ziehen und schlagwortartig über ein Thema informieren. Das Thema muss verkauft werden, weshalb die Kampagne ansprechend und professionell aufgebaut werden muss. Hier ist Phantasie gefragt und nicht nur ein weiteres Merkblatt am Anschlagbrett.

Fazit

Unser Sicherheitsbewusstsein ist zu gering. Den GMV im Umgang mit IT haben wir noch zu wenig entwickelt. Dadurch sind wir und unsere IT-Infrastrukturen verwundbar. Das Potenzial der Anwender ist zugunsten der IT-Sicherheit zu nutzen. Hierfür sind umfassende Anstrengungen zwingend nötig, welche von allen Beteiligten getragen werden müssen. ■

Ausstellung cybernetguard

Die Hochschule für Wirtschaft Luzern hat im Verkehrshaus der Schweiz gemeinsam mit Microsoft und verschiedenen weiteren Partnern eine umfassende Ausstellung zum Thema Computersicherheit und Privatsphäre entwickelt. Das Ziel der Ausstellung ist die Förderung der Awareness der Besuchenden. Die 3x3 Verhaltensregeln werden allgemein verständlich vermittelt. Weiter werden mit multimedialen Modulen die Gefahren und Schutzmöglichkeiten aufgezeigt. Weitere Details unter www.cybernetguard.ch