SSI-Bulletin 2/01

Das Mitteilungsorgan der Schweizerischen Vereinigung unabhängiger Sicherheitsingenieure und -berater

Nicht ohne Awareness

Wie kann die Informationssicherheit im Unternehmen gewährleistet werden? Tatsache ist, dass jede Lösung nur so gut ist wie das Sicherheitsbewusstsein des Managements und der Mitarbeitenden. Eine gesunde Awareness muss Teil der Unternehmenskultur sein; sie kann nicht durch Einzelaktionen erreicht werden. Methoden zur Sensibilisierung sind gefragter denn je.

Awareness durch interaktive Einbindung der Mitarbeitenden (Szene aus dem Web Based Training «SAVE»).

Von Markus Herren

«Sicherheit? – Bitte nicht schon wieder! Verschonen Sie mich damit, dafür habe ich keine Zeit, das überlasse ich unseren technischen Spezialisten. Und überhaupt: Sicherheit bringt doch nichts als Kosten mit sich. Bei uns ist schliesslich noch nie etwas passiert, wir haben es ja relativ gut im Griff. Was soll also die mühsame Übung?»

So und ähnlich tönt es oft, wenn es um die Einführung neuer Massnahmen im Bereich der Informationssicherheit geht. Sicherheit wird als Thema für Ängstliche oder für Wichtigtuer angesehen. Für die Mitarbeitenden im Unternehmen ist der Nutzen von Sicherheitsmassnahmen tatsächlich nicht immer offensichtlich. Vermeintlich repressive Vorschriften und technische Einschränkungen hinterlassen meist einen stärkeren Eindruck als die dadurch erreichte Gewissheit eines hohen Sicherheitsniveaus.

Selbst Führungskräfte tun sich mitunter schwer mit der realistischen Einschätzung der möglichen Gefahren und von deren Auswirkungen für ihr Unternehmen. Die momentane Produktivität, Effizienz und Flexibilität liegt ihnen verständlicherweise näher als die Reduktion von scheinbar rein theoretischen Risiken.

Bedeutung der Awareness

Durch das Bewusstsein alleine wird die Informationsverarbeitung natürlich noch nicht sicher. Technische (Firewall, Virenschutz, Verschlüsselung, Backup usw.), organisatorische (Wartung, Zugriffskontrolle, Alarmbereitschaft usw.) und physische Massnahmen (Brandschutz, Schliessung, sichere Infrastruktur usw.) sollen selbstverständlich nach klaren Konzepten zum Einsatz kommen. Die Wirksamkeit all dieser Massnahmen kommt aber erst durch die funktionsgerechte Eigenverantwortung der Mitarbeitenden aller Stufen voll zum Tragen. Andernfalls werden die erarbeiteten Sicherheitskonzepte nur zögernd umgesetzt, schlecht eingehalten, nach Möglichkeit umgangen, nie aktualisiert. Auf diese Weise verkümmern sie rasch zum kaum beachteten Ladenhüter.

In verschiedenen Umfragen zur Informationssicherheit wird das Fehlverhalten des eigenen Personals als Gefahr Nummer eins eingestuft. Dies nicht nur im subjektiven Empfinden, sondern auch in Bezug auf tatsächlich erlittene Schäden. Immer wieder erreichen uns Nachrichten von Virenverseuchungen, lahm gelegten Diensten, Informationsdiebstahl oder mangelhaft geschützten Daten, und praktisch immer haben menschliche Fehler, sei es aus Nachlässigkeit oder Unwissen, zum Unglück beigetragen.

Der amerikanische IT-Experte Patrick McBride fordert in einem Essay, von jedem Sicherheits-Dollar 40 Cents (!) für Aware-

Lesen Sie weiter auf Seite 2

Fortsetzung von Seite 1

ness einzusetzen. Das schwächste Glied in der Sicherheitskette ist und bleibt der Mensch. Falls er sich seiner wichtigen Rolle nicht bewusst ist, wird er trotz ausgefeilter Technologie unabsichtlich zum Helfer von Hackern, Crackern und Spionen.

Bewusstseinsbildung

«Tell me and I forget, teach me and I remember, involve me and I learn!» Diesen Leitsatz, den schon die alten Römer sinngemäss kannten, haben wir beim Erarbeiten von Awareness-Programmen stets im Hinterkopf. Gerade im Security-Bereich ist die Lernbereitschaft oft nicht besonders ausgeprägt, weil der unmittelbare persönliche Nutzen, anders als etwa bei der Einführung neuer Anwendungssoftware, nicht vorhanden ist. Wie können wir also Mitarbeiter in ein Sicherheitsprogramm einbeziehen?

Aus einer langweiligen Pflichtübung muss spannende Unterhaltung werden, die Vermittlung von Informationen muss möglichst interaktiv sein. Das Sicherheitsbewusstsein der Mitarbeitenden muss in Fleisch und Blut übergehen, und dies möglichst ohne Zuhilfenahme von aufgebauschten «Horror»-Szenarien. Sicherheit soll zu einem möglichst positiv behafteten Begriff werden und uns überall hin als Selbstverständlichkeit begleiten.

Rahmenbedingungen schaffen

Awareness beginnt damit, dass das Erreichen und Aufrechterhalten eines definierten Sicherheitsniveaus von der Geschäftsleitung als strategisch erklärt wird. Für die konkrete Umsetzung der Sicherheitsgrundsätze müssen sodann unternehmensweit gültige Konzepte und Richtlinien geschaffen werden.

In der Aufbauphase eines umfassenden Information Security Managements hat sich unserer Erfahrung nach die Durchführung von Risiko-Workshops für Linien-Vorgesetzte und IT-Verantwortliche als sehr zweckmässig erwiesen. Nicht nur das intensive Befassen mit Sicherheitsfragen, sondern auch der Übergang vom massnahmenorientierten zum risikoorientierten Denken tragen zur Awareness auf dieser Stufe bei. Wer Risiken beurteilen kann und sich somit der Bedeutung der Informationssicherheit bewusst ist, erfüllt automatisch eine Vorbildfunktion gegenüber den Mitarbeitenden und hilft auf diese Weise mit, die Sicherheitskonzepte nach innen zu vermarkten.

Zu den günstigen Rahmenbedingungen gehört im Weiteren ein effizienter Informatik-Support. Damit soll gewährleistet werden, dass Probleme rasch erkannt und behoben werden können. Zudem hält eine zuvorkommende Kontaktstelle die IT-User eher vor sicherheitskritischen Eigenbasteleien und inoffiziellen Lösungen ab.

Aufmerksamkeit gewinnen

«Stell dir vor es gibt neue Sicherheitsinfos, und keiner merkt's.»

Ganz klar, eine Botschaft kann erst vermittelt werden, wenn die Aufmerksamkeit da ist. Zum Gewinnen dieser Aufmerksamkeit bestehen erfahrungsgemäss folgende Möglichkeiten: Schaffen einer Identität für Informationssicherheit (z. B. Logo, Slogan, Comic-Figur), allgegenwärtiges Erscheinen des Themas (z. B. Mausmatten, Bildschirmschoner, Plakate) und «Zückerchen» anbieten (z. B. Emergency Kit, Wettbewerb, Kugelschreiber).

Interesse wecken

Um die Mitarbeitenden für Informationssicherheit zu sensibilisieren, schlagen wir periodische Informations-Kampagnen im Sinne von «Sicherheitstagen» vor. Dazu gehören beispielsweise ein Informationsstand an einer gut frequentierten Stelle, ein Artikel zu einem IT-Sicherheitsthema in der Hauszeitung und das Verteilen von ansprechend aufgemachten Merkblättern.

Im Sinne der bereits beschriebenen Anforderungen an die Bewusstseinsbildung ist das interaktive Einbinden des Zielpublikums ein Muss. Mit einem Web

Editorial

Die Informationstechnologie hat sich in den letzten Jahren rasant entwickelt. Heute besteht unsere Informationsinfrastruktur aus Millionen von Datenleitungen, Computernetzwerken und kabellosen Verbindungen, die Rechenzentren, Computernetzwerke und Steuerungszentralen verbinden und mit Informationen versorgen (Sprache, Daten und Bilder). In verschiedenen westlichen Ländern ist nach beunruhigenden Tests der Schutz der Basis-Infrastruktur von Computernetzen zur nationalen Aufgabe erklärt worden. In der Schweiz ist man davon noch weit entfernt.

Die Informationsinfrastruktur ist verletzlich, weil sie gross, komplex, vernetzt und fragmentiert ist und rasant wächst. Insbesondere die Bereiche Telekommunikation, Elektrizität und computergestützte Netzwerke sind wichtig, da sie die Basis für das Funktionieren der übrigen zentralen Infrastrukturen bilden. Nicht zuletzt führen in allen diesen Sektoren Rationalisierungs- und Privatisierungsmassnahmen dazu, dass auch die Steuerungsprozesse der technischen Systeme konzentriert werden.

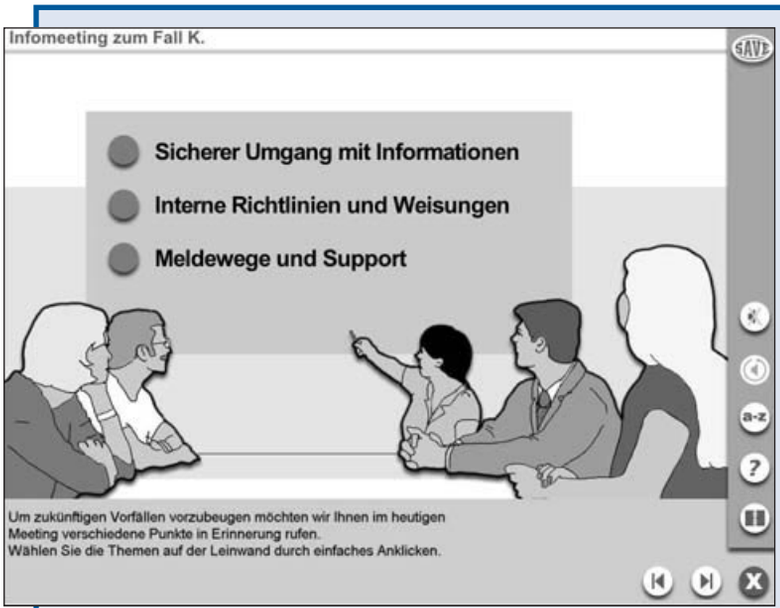
In den einzelnen Infrastruktursektoren bestehen in unterschiedlichem Ausmass konzeptionelle, organisatorische und technische Schutzmassnahmen. Den für die Netzwerksicherheit zuständigen Fachleuten Untätigkeit vorzuwerfen, wäre unlauter. Die Ansätze sind jedoch bis heute vor allem Insellösungen, welche die zunehmende Vernetzung zwischen den Systemen, die Privatisierung der Infrastrukturen und die Verwischung der staatlichen Grenzen noch kaum im Auge haben. Es reicht nicht, einfach jedes System mit Anschluss an ein öffentliches Netz mit einer Eintrittsschranke zu versehen. Viel mehr Gewicht muss der Funktion der Systeme zukommen. Bis heute ist die notwendige Sensibilisierung für die Problematik noch zu gering.

Der aus heutiger Sicht und mit Blick auf das Ausland Erfolg versprechendste Ansatz zur Sicherung der Informationsinfrastrukturen und zur Aufrechterhaltung und Verstärkung des Vertrauens bildet die Partnerschaft von Staat und Privatwirtschaft. Sicherheitsstrategien für den Schutz von Elektrizitäts- und Telekommunikationsnetzen, Finanztransaktionssystemen, für Leit- und Kontrollsysteme der Transportinfrastruktur können nur angegangen werden, wenn Betreiber, Benützer und Aufsichtsbehörden gemeinsam vorgehen.

Daniel Bircher

Zum Autor

Markus Herren ist promovierter Naturwissenschafter (Dr. phil. nat.), Sicherheitsberater SSI und Leiter des Fachbereichs Informatiksicherheit bei BDS AG in Bern.



Awareness durch klar kommunizierte Konzepte (Szene aus dem Web Based Training «SAVE»).

Awareness durch verständliche Information (Szene aus dem Web Based Training «SAVE»).

Based Training, das den Anwendern die Gelegenheit gibt, sich individuell und auf spielerische Weise in die Verhaltensregeln für die Informationssicherheit einzuarbeiten, werden nachweislich gute Resultate erzielt.

Informieren

Das einmal geweckte Interesse soll natürlich nicht gleich wieder verloren gehen. Deshalb ist es wichtig, Informationen zu Gefahren und richtigem Verhalten dauerhaft anzubieten. Als permanente Informationsplattform für Fragen der Informationssicherheit bietet sich naturgemäss das Intranet an. Ergänzend zu den unter Umständen relativ «trockenen» Facts stellen Bilder, interaktive Tests und Nachschlagemöglichkeiten in Lernprogrammen einen Mehrwert dar, der sehr geschätzt wird.

In einem sicherheitsbewussten Unternehmen haben die Mitarbeitenden jederzeit die gültigen Verhaltensrichtlinien zur Verfügung. Zudem kennen sie ihre Kontaktstellen für Sicherheitsfragen sowohl im Bereich der elektronischen als auch der nichtelektronischen Informationen und Daten.

Aktuelle Information und effiziente Kommunikation tragen wesentlich zur Awareness im Unternehmen bei.

Fazit

Awareness bildet einen Grundpfeiler der Informationssicherheit. Ein optimales Sicherheitsbewusstsein im Unternehmen wird durch eine permanente Kombination von Information, Ausbildung und Special Events erreicht. Die Mitarbeitenden müssen auf möglichst motivierende Art in den Sicherheitsprozess einbezogen werden.

SSI-Mitgliedsfirmen stellen sich vor:

Gruner AG

Die Gruner AG Ingenieure und Planer mit Hauptsitz in Basel ist führend in der Bau-, Umwelt-, Haustechnik- und Energieplanung. Die Tätigkeitsbereiche umfassen neben den klassischen Ingenieurdienstleistungen auch Generalplaner- und Berateraufgaben im Hochbau und im Infrastrukturbereich, Sicherheitsberatungen, Bauerneuerungsaufgaben, Projektmanagement- und Controllingaufgaben. Die Gruner AG verfügt in der Schweiz über einen Mitarbeiterstab von rund 170 Fachleuten. Je nach Aufgabenstellung werden für die Bearbeitung von Projekten kompetente interdisziplinäre Projektteams gebildet.

Unsere Dienstleistungen im Bereich Sicherheit

- Sicherheitsanalyse, Risikoermittlung, Kurzbericht StFV, Einsatzplanungen bei Chemieanlagen, Strassen und Eisenbahnen
- Sicherheitskonzepte, -ordner, Ausbildung bei Hotels, Industrien, Gewerbe, öffentlichen Institutionen
- Brandschutzkonzepte, Computersimulation, Brand, Rauch, Flucht
- Sicherheit von Bauwerken (Explosion, Brand, Erdbeben, Schnee)
- Arbeitssicherheit, Branchenlösung, Ausbildung
- Lebensmittelsicherheit
- Securitykonzepte bei öffentlichen Institutionen, Dienstleistungsbetrieben

Adresse: Gruner AG
Ingenieure und Planer
Gellerstrasse 55, Postfach
CH-4020 Basel
Tel. 061 317 61 61
Fax 061 271 79 48
www.gruner.ch

Kontakt: Herr Ulrich G. Stiefel
Tel. 061 317 64 28
E-Mail ulrich.stiefel@gruner.ch

Herr Dr. Alex Scheiwiller
Tel. 061 317 64 40
E-Mail alex.scheiwiller@gruner.ch

Sicherheit 2001: Grösster deutschsprachiger Sicherheits-Fachkongress

SSI-Tagungen erfreuen sich immer über grossen Besucheraufmarsch.

Traditionell findet zur «Sicherheit» der begleitende Fachkongress statt, die so genannte «Informationstagung», die von der SSI in Zusammenarbeit mit weiteren Verbänden und der MediaSec AG organisiert wird. Zahlreiche Sicherheitsexperten aus dem In- und Ausland beleuchten während eines halben Tages ein Thema aus dem weitläufigen Gebiet der Sicherheit. Mit 15 verschiedenen Halbtagsmodulen ist die Informationstagung 01 die grösste Fachtagung, die je parallel zu einer deutschsprachigen Messe stattgefunden hat. Nachdem die Veranstaltung jahrelang im Stadthof 11 durchgeführt wurde, findet die Informationstagung neu in der Halle 7 direkt im Messegebäude statt. Die Besucherinnen und Besucher profitieren von einer verbesserten Infrastruktur und können Messe und Kongress jetzt bequem unter einem Dach besuchen.

Unternehmenssicherheit wird heute als umfassender, integrierter Teil von Managementsystemen und Prozessen verstanden. Diese werden durch technische Systeme, organisatorische Massnahmen und Sicherheitsausbildung unterstützt. In den letzten Jahren haben sich die Bereiche der Sicherheit erweitert. Dies ist einerseits auf die veränderte Bedrohungslage, also die konkrete Gefährdungssituation einer Unternehmung, und andererseits auf deren erhöhte Verletzbarkeit im Bereich der Anlagen und Funktionen zurückzuführen. Den optimalen Sicherheitsansatz in einer Unternehmung zu finden, erfordert deshalb auch vermehrt ganzheitliches Denken: Wirtschaftlichkeit, Nachhaltigkeit, Akzeptanz und Zielorientierung sind in diesem Zusammenhang keine Schlagworte, sondern echte Herausforderung.

Die Tagung wird mit einer Analyse zur aktuellen Sicherheitslage und zu spezifisch übergeordneten Sicherheitsthemen der Wirtschaft wie IT, Wirtschaftsdelikte und Kriminalität unter Berücksichtigung der politischen Ereignisse eröffnet. In nachfolgenden Halbtagesmodulen werden die Fachgebiete vertieft. Prävention und Abwehr in organisatorischen und technischen Bereichen stehen im Vordergrund.

An den Veranstaltungen für Arbeitssicherheit und Gesundheitsschutz werden ergänzende Themen zu Absentismus, Luftschadstoffen und Schutzausrüstung behandelt. Im Sinne eines Sicherheitsdaches in der Unternehmung sind Managementsysteme von zentraler Bedeutung. Hier wiederum schliesst sich der Kreis zum Security-Bereich. Die Informationstagung Sicherheit 2001 bietet mit 85 praxisbezogenen und erfahrenen Referenten wiederum einen umfassenden Überblick über die wichtigsten und aktuellsten Bereiche der Sicherheit und des Risikomanagements. In der Agenda eintragen: vom 13.11. bis 16.11.2001 in der Messe Zürich, in Zürich.

Das detaillierte Tagungsprogramm ist erhältlich bei:
MediaSec AG
Tägernstrasse 1
8127 Forch/Zürich
Telefon +41 (0)1 980 44 66
Fax +41 (0)1 980 66 67
E-Mail info@mediasec.ch.
Online-Informationen und Online-Anmeldung unter www.mediasec.ch

Themen 2001

Aktuelle Bedrohung von Gesellschaft und Wirtschaft
Brandschutz
Personenschutz
Einbruchschutz und Alarmierung
IT-Sicherheit für KMU
Krisenmanagement und Notfallplanung
Sichere Rechenzentren und IT-Umgebung
Weniger Absenzen dank Prävention und Motivation
Facilitymanagement und Sicherheit
Zutrittskontrolle
Luftschadstoffe – Gefahrenstoffe im Arbeitsbereich
Managementsysteme und Sicherheit im Unternehmen
Persönliche Schutzausrüstungen
Brandschutz und moderne Bauten
Hightech-Security

I M P R E S S U M

Herausgeber:	Schweizerische Vereinigung unabhängiger Sicherheitsingenieure und -berater Güstrasse 46, CH-8700 Küsnacht Telefon 01 910 73 06, Fax 01 910 73 96
Erscheinungsweise:	Drei Ausgaben pro Jahr
Mitarbeiter dieser Ausgabe:	Markus Herren, Dr. phil. nat, BDS AG, Bern Daniel Bircher, Ernst Basler + Partner, Zürich Ulrich G. Stiefel, Gruner AG, Basel
Layout, Satz und Lithos:	WPS-RCM AG, CH-8954 Geroldswil
Druck:	buag Grafisches Unternehmen AG, CH-5400 Baden-Dättwil