Interview mit Wolfgang Sidler,
CEO Swiss IT-Markt AG

Stichhaltige Security-Konzepte erhöhen Kreditwürdigkeit

Der Ko-Autor der Publikation «Sicherheitshandbuch», Wolfgang Sidler, war sechs Jahre lang als Sicherheitsbeauftragter der Bank Julius Bär tätig. Seit kurzem sitzt er auf dem CEO-Stuhl der Swiss IT-Markt AG. Sidler gilt als Spezialist für «Security-Awareness». ICT kommunikation traf ihn am diesjährigen bw-digitronik-Security-Day in Regensdorf und unterhielt sich mit ihm über aktuelle Fragen der Informatiksicherheit.

Mit Wolfgang Sidler sprach Karlheinz Pichler

ICT kommunikation
Herr Sidler, Sie übten bei der Bank Julius Bär mehrere Jahre lang die Funktion eines IT-Security Officers aus. Hat sich Ihr Engagement für diese Bank ausgezahlt? Oder anders gefragt: Ist es für ein Unternehmen heute generell notwendig, einen eigenen Sicherheitsverantwortlichen anzustellen?
Wolfgang Sidler: Die sechs Jahre als IT-Security Officer bei der renommierten Schweizer Privatbank Julius Bär in New York und Zürich haben mir sehr viel Erfahrung und Know-how auf dem Gebiet der IT-Sicherheit gebracht. Sicherheit ist nicht gratis. Jedes Unternehmen, klein oder gross, braucht IT-Sicherheit. Nur kann sich nicht jedes Unternehmen einen Vollzeit-Security-Officer leisten. Ich propagiere deshalb das Modell des IT-Security Officers auf Zeit. Das heisst, Sie mieten sich einen IT-Security-Spezialisten auf Zeit, z. B. einen Tag pro Woche oder pro Monat. Dieser löst Ihnen die anstehenden Sicherheits-Herausforderungen.

Waren Sie in dieser Zeit bei der Bank Bär mit konkreten Bedrohungsszenarien konfrontiert?
Wie jedes international tätige Bank-Unternehmen, waren auch wir Ziel von verschiedenen Angriffen. Jedoch sind wir nie von Phishing-Attacken bedroht worden, da wir keine Retail-Bank sind und Kunden keine Zahlungen online tätigen können. Dafür wurden Notebooks gestohlen. Deren Festplatten waren jedoch verschlüsselt, und somit erlitten wir ausser dem materiellen Schaden keine ernsthafte Bedrohung. Auch wurde versucht, unsere Web-Seite zu verändern, was den Hackern jedoch nicht gelungen ist.

Worin liegen Ihrer Meinung nach heute die grössten IT-Security-Herausforderungen für KMU?
Die grösste Herausforderung liegt darin, die Risiken für das eigene Unternehmen zu kennen. Sie müssen Ihre Geschäftsprozesse und deren Abhängigkeiten zu den Applikationen und IT-Systemen kennen. Ich habe auch die Erfahrung gemacht, dass sich das Management der eigenen Verantwortung nicht bewusst ist. Das Management sollte eigentlich wissen, dass diese Sicherheitsverantwortung

+ + + NEWSTICKER + + + NEWSTICKER + + + NEWSTICKER + + +

VIRUS ATTACKIERT WINDOWS UND LINUX
In den Labors von Kaspersky Antivirus ist ein neuer Cross-Plattform-Virus aufgetaucht. Der Schädling mit den Namen Virus.Linux.Bi.a beziehungsweise Virus.Win32.Bi.a ist in Assembler programmiert und kann nur das aktuelle Datenverzeichnis angreifen. Allerdings kann der Virus Dateien in beiden Formaten, die Windows und Linux verwenden, ELF und PE, attackieren.

MICROSOFT REPARIERT IE-SCHWACHSTELLE
Das Warten für sicherheitsbewusste Internet-Explorer-Anwender hat ein Ende. Mehr als zwei Wochen nachdem eine als extrem kritisch eingestufte Sicherheitslücke öffentlich bekannt geworden war, nutzte Microsoft seinen regulären Patch-Day für den Monat April unter anderem dafür, die Schwachstelle zu kitten.

IBM VERSCHLÜSSELT MIKROPROZESSOREN
IBM hat eine neue Verschlüsselungstechnologie angekündigt, die Elektronikprodukte vor Datenmissbrauch schützen soll. Die unter dem Namen «Secure Blue» von IBM Research entwickelte Technologie basiert auf einer Hardware-Lösung, die in Mikroprozessoren-Chips integriert werden kann. Damit will IBM sicherheitstechnische Standards für mittel- und niedrigpreisige Endgeräte ermöglichen, die bisher nur von Mainframes in leistungsstarken Rechenzentren erreicht werden konnten.

MALWARE-SCHUTZ FÜR GRISOFT
Angesichts zunehmender Gefahr durch Schädlinge jenseits von Viren und Würmern will der tschechische Anti-Viren-spezialist Grisoft seine Produktpalette um einen umfassenden Malware-Schutz erweitern. Die Übernahme des deutschen Anti-Malware-Entwicklers ewido networks ist für den Hersteller der Sicherheitssoftware AVG Anti-Virus ein weiterer Schritt auf dem Weg zu einer kompletten Anti-Malware-Schutzlösung.
(ICT/pressetext)

Interview mit
Wolfgang Sidler,
CEO Swiss IT-Markt AG

nicht delegiert werden kann. IT-Sicherheit ist Chefsache! Die Geschäftsleitung muss einen klar definierten Auftrag an den IT-Security Officer, Informatik-Leiter oder einen externen IT-Security-Spezialisten erteilen. Es gilt auch, alle Mitarbeiter zum Thema IT-Sicherheit zu sensibilisieren. Ich kann nur empfehlen, das Unternehmen einem Security-Audit (First-Cut-Review) durch einen unabhängigen IT-Security-Berater unterziehen zu lassen. Diese Investition gibt einen Überblick über den Sicherheitszustand eines Unternehmens in Hinblick auf Management, Organisation, Recht und Technik und zeigt klar die Schwachstellen auf. Anhand dieser Schwachstellen-Analyse können dann Schritt für Schritt Lösungen zur Verminderung der Risiken in Angriff genommen werden.

Sie gelten als Fachmann für Awareness. Laut einer Studie der FGsec bestätigen 77 Prozent der CISO (Chief Information Security Officer) heute den Nutzen eine Sicherheitskultur. Woran liegt es, dass nach den Viren und Würmern die Mitarbeiter eines Betriebes immer noch als grösste Bedrohung für die Sicherheit eingestuft werden?
Über Viren, Würmer, Spyware und Phishing-Attacken wird fast jeden Tag offline oder online berichtet. Weil über die anderen Sicherheits-Bedrohungen in den Medien wenig berichtet wird, ist die Wahrnehmung nicht gross genug. Dass vertrauliche Dokumente anstatt geschreddert zu werden, einfach sorglos zum Altpapier gelegt werden, CDs mit sensitivem Inhalt achtlos weggeworfen werden, PCs mit vertraulichem Inhalt an einen IT-Provider zur Reparatur geschickt werden etc. beweist, dass viele Sicherheits-Risiken mit wenig Aufwand, einer Weisung und mit einer einfachen Sicherheits-Kampagne verhindert werden können. Ein verständlicher Sicherheits-Leitfaden für alle Mitarbeiter kann Wunder bewirken.

Gibt es in der Praxis noch andere Mittel, um das Bewusstsein der Angestellten für Sicherheitsbelange drastisch zu erhöhen und die Sicherheitskultur sozusagen zu verinnerlichen?
Bei der Bank Julius Bär haben wir letztes Jahr eine zweistufige Sicherheits-Kampagne durchgeführt. In einer ersten Phase haben wir allen Mitarbeitern eine CD mit einem Viren-Scanner und anderen nützlichen Security-Tools inkl. Booklet mit Tipps zum Surfen, Spam, Wireless LAN, Dialer, E-Mail, Online-Banking und einem IT-Lexikon geschenkt. In der zweiten Phase haben wir einen Sicherheits-Leitfaden zum sicheren Umgang mit Kunden- und Geschäftsdaten in Deutsch und English an alle Mitarbeiter verteilt. Diese Aktion war ein Erfolg und wurde von den Mitarbeitern mit einem guten Feedback belohnt. Mit etwas Know-how und mit einer guten Idee muss Sicherheit nicht unbedingt teuer sein.

Viele Sicherheitsverantwortliche fordern, dass Security vom obersten Management mitgetragen werden müsse. Das vermittelt den Eindruck, als ob im Top-Management dieses Bewusstsein genauso fehlt wie in den unteren Hierarchieregionen. Ist dies in der Praxis so?
Viele Manager ignorieren einfach die Risiken. Denn wenn sie die Risiken kennen würden, müssten sie etwas dagegen unternehmen und dies bindet Ressourcen und verursacht Kosten. Auch Aussagen wie «Wer will denn bei mir was stehlen?» oder «Wieso soll gerade bei mir eingebrochen werden?» sind häufig anzutreffen. Verluste werden nicht immer durch externe Bedrohungen verursacht. Viele Fehler geschehen durch Fehlmanipulationen, Unwissenheit, Unachtsamkeit, Sorglosigkeit und immer mehr auch durch Sabotage. Vergessen Sie nicht, dass auch Wirtschaftsspionage ein aktuelles Thema ist. Speziell kleine und mittelgrosse Unternehmen haben viel Know-how, das einfach gestohlen werden kann.

Kann denn nur Druck von aussen, etwa durch den Gesetzgeber oder durch den Wettbewerb, die Manager dazu bewegen, mehr in IT-Sicherheit zu investieren oder wenigsten der IT-Sicherheit mehr Beachtung zu schenken?
Heute ist es üblich und auch von Gesetzes wegen vorgeschrieben, dass die Buchhaltung einer Aktiengesellschaft jährlich von einer Revisionsstelle kontrolliert werden muss. Vielleicht wird es noch Jahre dauern, bis dieses Vorgehen auch auf dem Gebiet der IT-Sicherheit zur Usanz wird. Ein Trend ist für mich klar: IT-Compliance, IT-Governance und IT-Sicherheits-Zertifizierungen werden in den nächsten Jahren in Europa und in der Schweiz zunehmen. Hat ein Unternehmen gemäss Basel II alle IT-Prozesse und IT-Systeme unter Kontrolle und sind diese sicher, wird es eine bessere Kreditwürdigkeit erhalten.

Welche zusätzlichen Massnahmen sind nötig, um die schwindende Grenze zwischen betrieblichem und öffentlichem Umfeld für die Firmen sicher zu gestalten?
Die derzeitige wie künftige Mobilität, sei es mit Blackberry, Smartphones oder Notebooks, lässt die Grenzen von Geschäfts- und Privatsphäre zunehmend schwinden. Es ist eine enorme Herausforderung für die Sicherheits-Verantwortlichen, diese Grenze zu definieren und auch in einem zulässigen Masse zu überwachen. Es gibt Technologien und Lösungen, die neu, aber noch nicht ausgereift sind. Ich kann nur an ein durchdachtes Vorgehen appellieren, wenn Unternehmen solche Technologien einsetzen. Sie sollten auf jeden Fall Standardlösungen verwenden, die der heutigen Best-Practice entsprechen. Damit haben sie auch die Möglichkeit, sich mit andern ihrer Branche zu messen (Benchmarking). ■