

Sicherheit rentiert

ONLINE-LÖSUNGEN Security sollte nicht nur IT-Budget-Faktor sein, sondern als Imageschutz eines Unternehmens bewertet werden.

STEFAN ARN

Das sich Sicherheit betriebswirtschaftlich lohnt und kein Luxus ist, haben Anfang Jahr weltweit Aufsehen erregende Cyberangriffe auf Banken und Kreditkarteninstitute bewiesen. Mit Hilfe gefälschter E-Mails und Web-Seiten gelang es einer osteuropäischen Täterschaft, verschiedentlich in den Besitz von Zugangscodes von Konten zweier Kantonalbanken zu kommen: Online-Kunden wurden zur Herausgabe ihrer Vertrags- und Streichlistenummern sowie ihres Passworts verleitet. Die Täterschaft konnte sich damit den direkten Zugang auf Konten verschaffen und Geldüberweisungen auslösen. Der Schaden wurde nie genau beziffert.

Folgeschäden sind enorm

Image- und andere Folgeschäden sind enorm und kaum wirklich zu beziffern. Durch die gesteigerte Unsicherheit der Kundschaft einerseits und die erhöhte Intransparenz bei der Berechnung von Restrisiken bei den Entscheidungsträgern der Unternehmen andererseits, dürften sich mehrere geplante Online-Migrationsprojekte von Firmen anderer Unternehmensbereiche zeitlich verzögern.

Doch Security ist durchaus zuverlässig einsetzbar. Sie ist zwar eine komplexe Engineering-Aufga-

be, deren Einbindung in ein IT-System meist mehrere Jahre beansprucht. Doch wie die Schadensfälle zeigen, ist Sicherheit kein Luxus, will man Online-Lösungen anbieten. Soll ein abgesichertes System wie eine Versicherungspolice wirken, verlangt es gewisse Vorausinvestitionen. Diese zahlen sich aber rasch einmal aus und werden bezifferbar, wenn ein Unternehmen den Vorteil eines gesicherten E-Kanals voll nutzen kann.

Dazu bedingen sich aber Datensicherheit und die Möglichkeit, bei einem System alle einzelnen Bedienungsschritte transparent nachvollziehen zu können. Dies garantiert erstens, dass jeder einzelne Fall berechenbar bleibt. Zweitens, dass alle Bedrohungsszenarien durchexerziert werden können. Da Sicherheit nur so gut ist wie das schwächste Glied, müssen bei der Entwicklung und Implementierung solcher Systeme alle Prozessschritte wohl aufeinander abgestimmt werden. Sicherheitsprojekte für grosse Firmen nehmen mehrere Jahre in Anspruch. Da «time to market» wie immer eine Rolle spielt, ist es wichtig, Security-Entwicklungen in einzelne Prozessschritte aufzuteilen. Allerdings müssen diese gut aufeinander abgestimmt sein.

Beispielsweise benutzt die UBS für das Online-Banking ein interaktives Autorisierungssystem, das derzeit auf dem Markt als teures,

aber als eines der am besten abgesicherten Einstiegssysteme gilt. Es verzichtet auf das Einloggen via Vertragsnummer, Passwort und Streichliste, indem ein Pincode jedes Mal neu dynamisch generiert wird und der bei Nichtbenutzen innerhalb weniger Sekunden verfällt. Die Lösung basiert auf einer Chipkarte. Zudem kam ein ausge-

Angriffe wurden simuliert und abgeblockt.

klügeltes Challenge-Response-Verfahren zur Authentisierung zum Zug, wobei das Zielsystem eine zufällig generierte Parole (Challenge) ausgibt. Der Nutzer, der sich gegenüber dem Zielsystem authentisieren möchte, antwortet mit einem passenden Gegenstück (Response). Das Verfahren ist der Verwendung herkömmlicher Passwörter weit überlegen, da zum einen jede Response nur für einen Zugriff gilt und Abhören einem Angreifer nicht hilft.

Datenschutzverletzung

Doch mit der Technik allein war es nicht getan. Sie muss mit einer umfassenden betriebsprozesslichen und wirtschaftlichen Strategie in eine entsprechende Si-

cherheitsumgebung eingebunden werden. Entscheidend war, dass die einzelnen Releasezyklen exakt aufeinander abgestimmt waren. Die eigentliche Software-Entwicklung nahm anderthalb Jahre in Anspruch. Das Projekt selbst war auf drei Jahre ausgelegt. Bei den Bedrohungsszenarien wurde ein Angriff mit derselben Technik, wie er bei den beiden Kantonalbanken zur Anwendung kam, durchexerziert und erfolgreich abgeblockt.

Das Fazit fällt viel versprechend aus. Zunächst: Security wird berechenbar. Und das in dem Sinn, dass zwar ein beschädigtes Image sich nie wirklich beziffern lässt, aber ein Schadensfall durch die Möglichkeit der vollständigen Nachvollziehbarkeit der einzelnen Prozessschritte erkenn- und damit berechenbar wird. Von der Nachvollziehbarkeit eines gesicherten Umfelds werden zudem auch Branchen profitieren, bei denen diese gesetzlich gefordert ist. Dazu zählt die Wahrung der Urheberschaft im Rahmen des Patentschutzes in der chemischen Industrie. Zu denken geben muss auch die Tatsache, dass im Gegensatz zum Bankenaufsichtsgesetz die Datenschutzverletzung einer Krankengeschichte bei Krankenkassen ein Officialdelikt ist.

Stefan Arn, Unternehmer des Jahres 2003, CEO AdNovum Informatik AG, Zürich.