

SECURITY

Vorsicht, Netzüberfall!

Die Welt der IT-Verantwortlichen in Banken dreht sich um die Sicherheit der Computer und Netzwerke. Denn fast alle Prozesse laufen IT-unterstützt ab, und in keiner anderen Branche sind Sicherheitsstandards so bedeutend.

➔ **Martin Schwer**

Ob sich manche Bankvorstände an die guten alten Panzerknacker erinnern und nach den drei „schweren Jungs“ zurücksehen, die mit Schweißgeräten und allerlei anderer „Hardware“ Onkel Dagoberts Tresor zu Leibe rückten, ist nicht bekannt. Angesichts der bestehenden Risiken bei Sicherheitslücken im Computersystem muten die gefährdeten Summen aus dem „Bruch“ in Entenhausen jedoch eher bescheiden an. So ist es kein Wunder, dass IT-Sicherheit integraler Bestandteil des Risikomanagements ist und auch der Gesetzgeber mit entsprechenden Vorgaben zum Schutz von Netzwerk, Datenbank & Co. reagiert hat.

DIE MITARBEITER SIND TEIL DES SICHERHEITSKONZEPTS

Diese Vorschriften stellen zum Beispiel klar, inwiefern die Institute aktive Maßnahmen für das Risikomanagement im IT-Bereich ergreifen müssen. Dazu gehören etwa spezielle Systeme und Software zur Überwachung und die ständige Weiterentwicklung der bestehenden Sicherheitsmechanismen. Auch die Mitarbeiter gehören ins Konzept. Für sie schreiben die Vorgaben beispielsweise Schulungen vor.

Wo es im Kundenverkehr etwa darum geht, Geldautomaten oder Online Banking vor Manipulation zu schützen, drehen sich die meisten Maßnahmen zur IT-Sicherheit vor allem um interne Abläufe. So dürfen

beispielsweise die Netzwerkstrukturen keine Lücken aufweisen und Ausfällen muss wirksam vorgebeugt werden. Überdies müssen unbefugte Zugriffe durch Mitarbeiter ausgeschlossen sein.

Gerade was die eigenen Beschäftigten angeht, besteht nach Angaben von Michael Frauen vom Sicherheitsanbieter RSA oftmals Nachholbedarf: „Es ist leider keine Seltenheit, dass Daten gewollt oder ungewollt über Laptops, USB-Sticks, PDAs oder per E-Mail den Bereich der gesicherten Informationsinfrastruktur verlassen und von verschiedenen internen und externen Nutzern verarbeitet werden.“

Ein weiterer „Klassiker“: Verlässt ein Mitarbeiter die Bank oder nur die Abteilung, werden die Berechtigungen für Netzwerke, Datenbanken und Software oftmals nicht der neuen Situation angepasst. Derartige Pannen ziehen selten weitreichende Konsequenzen nach sich, im Missbrauchsfall ist die mögliche Schadenhöhe jedoch riesig. Denn abgesehen vom materiellen Verlust entsteht ein Vertrauensverlust bei den Kunden. Und der lässt sich häufig nur schwer beziffern.

Für Michael Frauen führt daher kein Weg an einem umfassenden Sicherheitskonzept vorbei, das präventiv Risiken vermeidet: „Hier ist eine Information-Risk-Management-Strategie notwendig, die effektive Mittel zur Erkennung, Bewertung und Minderung der Risiken bereitstellt,

denen Informationen über ihren gesamten Lebenszyklus hinweg ausgesetzt sind.“ Ein solches Konzept zählt umso mehr, wenn etwa Handelssysteme im Spiel sind und einzelne Mitarbeiter hohe Beträge verantworten. Das Beispiel Société Générale mit den mutmaßlichen Betrügereien um den Mitarbeiter Jérôme Kerviel im vergangenen Winter wirft ein grelles Schlaglicht auf diese Problematik und zeigt auch, wie stark die IT-Sicherheit vom Funktionieren der allgemeinen Sicherheitsmechanismen abhängt.

Aber auch Fragen in Bereichen, in denen es nicht zwangsläufig um Einzelposten in Millionen- oder gar Milliardenhöhe geht, müssen IT-seitig abgebildet werden und damit in einem ganzheitlichen Sicherheitssystem Berücksichtigung finden. Zum Beispiel: Wiewerden Überweisungen gesteuert? Und ab welchem Betrag greift automatisch das Vier-Augen-Prinzip?

DIE BETROFFENE ABTEILUNG ENTSCHEIDET MIT

Ziel einer funktionierenden Sicherheitsarchitektur sollte es nach Ansicht von Ulrich Haumann, dem IT-Sicherheitsbeauftragten bei der HypoVereinsbank (HVB), vor allem sein, Risiken gezielt zu begegnen: „Sicherheitsmanagement ist gelebtes Risikomanagement.“ Haumann sieht daher seine Aufgabe weniger in der Risikominimierung als in der Risikooptimierung: „Die Abteilungen müssen ihr Sicherheitsniveau selbst festlegen, indem sie ihre Risiken spezifizieren.“ Mit Unterstützung von Haumanns Truppe wird dann entschieden, welche Sicherheitsmaßnahmen die jeweilige Abteilung benötigt. Maßstab dabei ist immer, ob Regelungen im konkreten Zusammenhang sinnvoll sind. Diese Konstruktion hilft zudem dabei, Ressourcen zu schonen. Insgesamt orientieren sich die Maßnahmen der HVB an internationalen Standards wie der ISO-Norm.



Regeln funktionieren nur dann, wenn sich die Mitarbeiter daran halten. Daher gilt es vielfach, einerseits die nötige Sensibilität zu erzeugen, andererseits durch Automatismen Gefahren bereits wirkungsvoll vorzubeugen. Das Sicherheitsbewusstsein der





Mitarbeiter schärft Haumann beispielsweise mit Awareness-Kampagnen im Intranet: „Wir verdeutlichen dabei etwa, wie mit Passwörtern umzugehen ist.“ Hier hat der Sicherheitsexperte die Erfahrung gemacht, dass die Leute einsichtig sind, wenn Gefahren erklärt werden. „Außerdem erleichtern private Erfahrungen wie der E-Mail-Spam die Überzeugungsarbeit.“

LÜCKEN DÜRFEN GAR NICHT ERST ENTSTEHEN

Dazu kommen Mechanismen, durch die Lücken erst gar nicht auftreten können. Beispiel ist die Verwaltung der Zugriffsberechtigungen: Bei der HVB läuft diese komplett über einen elektronischen Workflow-Prozess: „Berechtigungen werden über Prozesse automatisch auf Basis des im Personalverwaltungssystem hinterlegten Tätigkeitsschlüssels zugeordnet.“

Daneben werden die IT-Systeme der Geldinstitute jedoch auch von externen Faktoren bedroht. An erster Stelle stehen hier häufig die Netzwerke. Denn diese verbinden unterschiedliche Bereiche und Funktionseinheiten, aber auch deutschland- oder sogar weltweite Standorte. So benötigt jede Filiale, jeder Standort, aber auch jeder Mitarbeiterlaptop geeignete Schutzmaßnahmen, damit sich die Leitungen nicht anzapfen lassen.

FAZIT

Die Sicherheit der IT-Systeme ist ein Thema, das die gesamte Organisation eines Kreditinstitutes betrifft. Hier muss umfassend

↑ DIESE BEREICHE IN BANKEN SIND IT-SICHERHEITSRELEVANT

▶ Sicherheitskonzept

Wie wird auf eine Verletzung der Sicherheitspolitik reagiert? Welche Prozesse und Regelungen werden implementiert und wie dokumentiert oder überprüft?

▶ IT-Infrastruktur

Dabei geht es um die Beschaffung sowie Inventar und Betrieb von Hard- und Software. Auch Wartungs- und Reparaturarbeiten müssen geregelt werden.

▶ Datenträger

Wie geht das Institut mit schützenswerten Betriebsmitteln um? Wie sind Aus- und Notfälle geregelt und findet ein Continuity Management statt? Bestehen klare Vorgaben zur Datensicherung?

▶ Sicherheitsvorgaben

Wie sind Aufgaben und Funktionen aufgeteilt? Bestehen ausreichende Zugangsberechtigungen?

▶ Software

Wer übernimmt die Softwareentwicklung und wie wird die Sicherheit der Applikationen sichergestellt? Findet eine ausreichende Beratung und Schulung der Benutzer statt?

▶ Client Management

Wie sind IT-Arbeitsplätze organisiert, besteht ein ausreichender Schutz vor Viren sowie Zu- und Angriffen von außen?

Vorsorge getroffen werden, um Risiken wirkungsvoll begegnen zu können. So verwundert es nicht, dass die Verantwortung für die IT-Sicherheit häufig direkt an den Vorstand gekoppelt ist.

Intern müssen die Institute sicherstellen, dass jeder Mitarbeiter nur auf die Informationen zugreifen kann, die für ihn relevant sind. Bei Jobwechseln müssen auch die Berechtigungen entsprechend angepasst werden. Dazu kommen „banale“ Faktoren wie der Schutz von Servern vor äußeren Einflüssen, eine funktionierende Datensiche-

rung oder die Einhaltung von Sicherheitsstandards bei Releasewechseln. Anfällig sind zudem interne und externe Netzwerke, hier müssen Firewalls und verschlüsselte Verbindungen sensible Daten schützen. Denn klar ist: In wenigen Branchen geht es um derart sensible Daten wie im Bankgeschäft. Und nur in wenigen Angelegenheiten reagieren Kunden so empfindlich wie in Bezug auf ihr eigenes Geld. ↙



AUTOR: Martin Schwer ist freier Journalist in Köln.

