IT-Sicherheit

Ohne IT-Sicherheit geht nix

„Wenn eine IT-Panne das Bankgeheimnis abschafft" titelte unlängst eine große Tageszeitung: Kunden war nach dem Einloggen in das Online-Banking der Zugriff auf Konten anderer Kunden möglich. Der Fehler trat nach einem kurz zuvor eingespielten Update auf.

Erst einige Wochen vorher erwischte es eine andere große deutsche Bank. Ebenfalls nach einem Software-Update wurden auf Kundenkonten Abbuchungen doppelt angezeigt. Dies führte unter anderem dazu, dass Kunden kein Geld mehr zur Verfügung stand.

Im Frühjahr traf es die Sparkassengruppe. Die Transaktionsdaten der EC-Kartenzahlungen des Dienstleisters TeleCash wurden zwei Mal verarbeitet. So wurden die entsprechenden Bezahlvorgänge, die Kunden zuvor in Geschäften mit EC-Karte und PIN abgewickelt hatten, doppelt abgebucht.

Schlechte Nachrichten über, nennen wir es mal vorsichtig, „IT-Störungen" reißen nicht ab. Die Tagespresse nimmt Vorfälle dieser Art gerne als Schlagzeilen. Manch einer unkt, dass die Einschläge näher kommen, es sei letztlich nicht die Frage, „ob" etwas passiert, sondern „wann" es passiert.

Bei den drei vorgenannten Beispielen ist hervorzuheben, dass es sich bei keinem der Fälle um einen „Hacker-Angriff" handelte. Ursächlich waren interne, technische Probleme oder menschliche Fehlhandlungen. Fest steht: IT-Störungen dieser Art werden zunehmen.

Dies liegt an verschiedenen Faktoren.

- Die Banken treiben die Digitalisierung stark voran, um weiterhin wettbewerbsfähig zu bleiben. Einerseits erhofft die Branche sich von einer Prozessoptimierung – sei es nun im Vertrieb oder in der Marktfolge – eine bessere Kosteneffizienz. Andererseits fordert der Markt heute eine weitgehende Digitalisierung und den damit einhergehenden Komfort. Allein deshalb schon wächst die Bedeutung der IT und mit ihr die Bedeutung der IT-Sicherheit.
- Hinzu kommt, dass die Systeme, unter anderem auch die Kernbankenverfahren, spätestens seit der Finanzkrise schneller und häufiger an regulatorische Anforderungen angepasst werden müssen. Die Komplexität der IT-Anwendungen sowie deren Anforderungen steigen.

AUTOR UND ANSPRECHPARTNER

Michael Switalla
Stv. Bereichsleiter IT-Sicherheit & Datenschutz,
E-Mail: michael.switalla@geno-tec.de

Treten dann Fehler auf, treffen sie häufig gleich sehr viele Bankkunden und werden zudem auch schneller einer breiten Öffentlichkeit bekannt, unter anderem über die Verbreitung in sozialen Medien.

Nicht außer Acht lassen darf man zudem die Bedrohungslage hinsichtlich krimineller Angriffe auf die IT-Systeme der Banken.

In unserer Wissensgesellschaft sind Informationen ein wertvolles Gut. Hier kann eine rasante Entwicklung der verschiedenen Angriffsszenarien beobachtet werden. Vielschichtige Varianten wie Advanced Persistent Threats (APT), also fortgeschrittene und andauernde Bedrohungen, die auf sehr stark eingegrenzte Systeme und Netzwerke zielgerichtet einwirken, sind schwer zu erkennen und abzuwehren. Auch weitere Angriffe mittels Ransomware (auch bekannt als „Verschlüsselungstrojaner") können erheblichen Schaden verursachen.

Im IT-Sicherheitsmanagement gilt es, die Risiken aus der IT-Nutzung herauszuarbeiten und zu bewerten. Die Umsetzung des IT-Sicherheitskonzepts muss sowohl aktuelle als auch mögliche zukünftige Entwicklungen berücksichtigen, um ein belastbares Risikolagebild erstellen zu können. Dabei ist es unabdingbar, wenn auch sehr zeitaufwändig, umfänglich Informationen zu sammeln und auszuwerten. Hier helfen letztlich nur ein gutes Netzwerk und ein gemeinsames Vorgehen.

Auch wir als GenoTec entwickeln unsere Dienstleistungen stetig weiter, um im Schulterschluss mit unseren Kunden die IT – und damit auch immer mehr das Geschäftsmodell der Banken selbst – gegen Störungen, Pannen und Angriffe abzusichern. ▬