Cyber-Bedrohungen: So hat man als Bank die Risiken im Griff

Zürich, 17.11.2020

Schon einiges ist am Licht

«Weltweit gelieferte CH-Verschlüsselungsmaschinen beinhalten von Staaten benutzte Hintertüren». «Hackerangriffe auf Spitäler in Deutschland». «Verschlüsselte Daten und Lösegeldforderung bei Schweizer Eisenbahnhersteller». «Systemausfall beim Hersteller verhindert Datensynchronisation und Zahlungsmöglichkeit mit Fitnessuhren».

Fast schon regelmässig tauchen solche Meldungen in der Presse auf. Tatsache ist, dass neben System- und Betriebseinschränkungen oder -ausfällen, auch Kosten- und insbesondere Reputationsverluste einschneidende Folgen eines Angriffes solcher Art sein können. Doch mit einem Abschluss einer «Cyber-Versicherung», was oft empfohlen wird, ist es noch nicht getan.

Versuch, die IT zu schützen

Oft beobachten wir, dass als Konsequenz solcher von Pressemeldungen geschürten Unsicherheiten Aufträge an die bank-eigene IT resultieren:
Die eigenen Systeme mögen noch besser geschützt werden - bspw. mittels «Hardening» von Servern und Netzwerkgeräten wie auch mittels Überprüfung der Netzwerksicherheit (bspw. durch einen Audit auf Firewall-Regeln). Vielleicht mag ein solcher interner Auftrag tatsächlich ein besseres Sicherheitsgefühl geben. Es ist eine Tatsache, dass auch weitere Sicherheitsmechanismen, wie beispielsweise ein «Intrusion Detection System» (IDS), helfen, schon früh Angriffsversuche aufzudecken. Dies geschieht mittels Heuristiken oder künstlicher Intelligenz aufgrund von Anomalien im eigenen Netz und auf Servern. Wir empfehlen allen Banken dringlich, solche Massnahmen lückenlos umzusetzen.

Zudem werden möglicherweise in der eigenen Bank Cyber-Risiken bereits adressiert, bevor sie eintreten können. Dies kann bspw. mittels einer sogenannten “Three Lines of Defense”, also einem mehrstufigen Schutz, sichergestellt werden. Es ist ratsam, diesem «Approach» zu folgen: Der Betrieb der IT muss sicherstellen, dass die geforderten Sicherheitsmechanismen implementiert sind. Auch «Security Officers», die Änderungen an der Systemlandschaft überprüfen und den Betrieb unterstützen, dürfen nicht fehlen. Nicht zuletzt runden Inspektionen sowie interne und externe Audits den Umfang einer solchen «Security Governance» ab.

Es empfiehlt sich sehr, mit dem betrieblichen Business Continuity Management (BCM) über ein Desaster Recovery (DR) hinweg alle Cyber Security-Risiken proaktiv zu adressieren.

Was tun bei einem Angriff?

Falls trotz den oben erwähnten sicherheitstechnischen Massnahmen und Prozessen ein Hackerangriff erfolgreich ist, sollte auf eine vorbereitete Massnahmenplanung zurückgegriffen werden: Ein vorher zusammengestelltes Incident Response Team (IRT), das sowohl aus Server-/Netzwerk-Betreibern und -Engineers besteht, als auch aus Cyber Security Experten und Penetration Testern, identifiziert die Ursache eines Angriffs.

Falls ein sogenannter «Security Event» Tatsache wird heisst es nicht, dass eine Bank gleich Verluste erleiden muss. Anomalien im Verhalten von Systemen liefern bereits wertvolle Indizien, um frühzeitig auf Cyber-Gefahren reagieren zu können: Nachdem die Ursache gefunden wurde, ist es ratsam, alle Bereiche, wo der sogenannte «Security Breach» stattgefunden hatte, zu isolieren. In der Regel empfehlen wir, betroffene Server sofort vom Netz zu nehmen und danach den «Scope» des Security Events zuerst einmal genauer abzugrenzen. Wir haben beobachtetet, dass dies aufgrund der geschäftlichen und zeitlichen Dringlichkeit oft weggelassen wurde. Als Folge davon können später keine Analysen der Ursache (Forensik) gemacht werden.

Bedrohungen müssen aus unserer Sicht auf den Systemen isoliert, respektive unter Quarantäne gesetzt werden. Nur so wird man für spätere Angriffe gewappnet sein. Im Falle eines Angriffes denken wir, dass – je nach Ausmass - beispielsweise kompromittierte Accounts blockiert und bösartige Dateien oder Server komplett gelöscht werden sollten. Um den Betrieb wieder aufnehmen zu können, müssen – je nach Umfang des Angriffes – betroffene Systeme neu aufgesetzt und Daten von Backups wiederhergestellt werden, um dann wieder ein laufendes System wie zuvor zu haben. Wir empfehlen immer ein «Lessons Learned» durchzuführen, welches die IT-Sicherheit zu verbessern hilft.

Ferner gilt noch zu beachten, dass in der EU aufgrund der Datenschutzgrundverordnung (DSGVO) Melde- und Informationspflichten bestehen. In der Schweiz empfehlen wir, Angriffe der Melde- und Analysestelle Informationssicherung des Bundes (MELANI) zu melden.

Risiko Mitarbeitende

Die Vergangenheit hat gezeigt, dass Angriffe nicht nur übers Internet kommen: Defekte oder abgekaufte Endgeräte der Bank, Angriffe auf VPN-Verbindungen sowie Mitlesen von Bildschirminhalten und Tastenklicks im HomeOffice, in die Bank eingeschleuste elektronische Geräte («Warshipping»), Besitzübernahme von bestehenden Webcams wie auch Phishing, Social Engineering oder Sabotage durch Mitarbeitende sind Beispiele weiterer möglicher Angriffsvektoren auf die Bank. Neben technischen und organisatorischen Mechanismen ist es aus unserer Sicht wichtig, das Risiko «Mitarbeitende» mittigeren zu können: Durch Aufbau einer betriebsinternen «Informationssicherheits»-Kultur kann der Einfluss von Mitarbeiterverhalten verbessert werden.

In diesem Zusammenhang ist es ebenfalls wichtig zu verstehen, wie und wie stark das aktuelle Sicherheitsbewusstsein bei den Mitarbeitenden ist. Darauf aufbauend erfolgt eine strategische Planung, wie dieses – auch mit messbaren Mitarbeiterzielen – gestärkt werden kann. Wir empfehlen immer, Themen wie das Abholen des Managements, bank-interne Kommunikation und auch Schulungen («Awareness Trainings») bei der Planung zu berücksichtigen. Nach einer abgeschlossenen Planung erfolgt die entsprechende Umsetzung (Implemen-

tation): die Informationssicherheitskultur sollte nicht nur auf Papier bestehen, sondern auch gelebt werden. Dies geschieht nach unserer Erfahrung erfolgreicher mit Einholen des Commitments von allen Mitarbeitenden. Nicht zuletzt weisen wir häufig auf eine Nachevaluation hin: Auch Bedenken, die noch nicht adressiert sind, müssen in einem weiteren Planungszyklus neu aufgenommen und später ebenfalls umgesetzt werden.

Es gibt nicht nur Cyber-Risiken…

Cyber-Risiken sind tatsächlich zumeist unsichtbar und sind nur ein Beispiel dafür, was auf einem Bankweiten «Risk-Radar» nicht fehlen darf. Auf ein grundlegendes, vollumfängliches Risk-Management kann aus unserer Sicht in der heutigen Zeit nicht verzichtet werden.

Die Soranus AG unterstützt mit ihren Risk-Experten beim internen Risk-Check und bei der Detail-Analyse. Mit unseren starken Partnerschaften können wir «Ready-to-use»-Lösungen für ein internes Risk Controlling und Riskmanagement anbieten. Wenn die Risiken bekannt sind, folgt ein Massnahmenkatalog, bspw. um diese zu mittigeren oder zu eliminieren. Die erfahrenen Soranus Consultants helfen gerne bei der Planung und in der Ausführung, respektive bei der Umsetzung von Massnahmen.

Haben wir Ihr Interesse geweckt? Zögern Sie nicht, uns zu kontaktieren.

Martin Waldburger
Senior Consultant

- Über 20 Jahre praktische Erfahrung im Finanzdienstleistungs- sowie ICT-Bereich
- Ausgebildet und seit 25 Jahren involviert in der Konzeption, Analyse und Implementation von unzähligen IT-Security-Projekten
- Referent zum Thema Cyber Security
- Weitere Beratungsschwerpunkte im Bereich IT-Programm- und Projektmanagement im Bereich Zahlungsverkehr, Quality Management sowie IT-Sicherheit

SORANUS
BANKING DELIVERED.

Soranus AG
Hohlstrasse 560
CH-8048 Zürich
www.soranus.ch