STOPPT

Digitale Angriffe auf Banken passieren immer häufiger. Sie gefährden nicht nur die Guthaben der Kunden, sondern auch den Ruf der Finanzinstitute. Professorin Solange Ghernaouti analysiert das Phänomen und zeigt Möglichkeiten auf, sich dagegen zu wappnen.

Das Gespräch mit ihm führte Nejra Bazdarevic.

Prof. Solange Ghernaouti

Direktorin der Swiss Cybersecurity Advisory & Research Group
Fakultät der HEC an der Universität Lausanne
www.scarg.org

In den letzten zwölf Monaten wurden übermässig viele Cyberangriffe auf Bank- und Finanzinstitute beobachtet. Woran liegt das?
Die Öffentlichkeit beginnt damit, Cyberangriffe auf Bank- und Finanzinstitute als herausragend wichtiges Risiko für eine wirtschaftliche Destabilisierung und für die Rufschädigung der betroffenen Organisationen wahrzunehmen. Dazu kommt das Problem von Datenverlusten, das sich durch die digitalen Technologien verschärft hat. Allerdings sind solche Datenverluste in mehr als 60 Prozent der anerkannten Fälle auf interne Ursachen zurückzuführen, also auf illoyale Angestellte, die damit Profit erzielen oder es ihrem Arbeitgeber heimzahlen wollen.

Das Internet bringt die Institute und ihre Kunden näher zusammen und erleichtert ihnen die Interaktion. In demselben Masse reduziert es aber auch den Abstand der Cyberpiraten und sonstigen Cyberkriminellen. Digitale Kommunikation kann immer potenziell zu boshaften Zwecken umgeleitet werden. Es ist heute technisch unmöglich, den Datenschutz und den Nichtmissbrauch von Daten sowie die Echtheit des Datenaustausches zu 100 Prozent zu garantieren.

Das Risiko steigt mit der zunehmenden Anzahl von digitalen Praktiken. Wenn immer mehr Bank- und Finanztransaktionen über das Internet abgewickelt werden und es hierfür immer mehr und immer einfachere Möglichkeiten gibt, dann wird das Risiko für die Institute immer grösser. Der Preis, den wir für den breiteren Zugang zum Internet bezahlen (Webseiten, soziale Netzwerke, E-Mail, digitale Zahlungssysteme, Zahlung mit dem Handy, Kartenzahlung ohne Kontakt etc.), sind die vermehrten Risiken und Bedrohungen.

Ist für die Zukunft mit häufigeren Cyberattacken zu rechnen?
Es ist heute so, dass die Institute von diesen inhärent anfälligen Technologien häufig abhängig sind und damit ständig Cyberbedrohungen riskieren. Die Kriminellen kennen alle Angriffspunkte und können ihre Aktionen so optimieren. Es kann sich dabei um technische Schwachstellen im Softwarecode oder in den Algorithmen, um fehlerhafte Implementierungen, um Konzeptfehler oder auch um Fehler bei der Verwaltung oder Verwendung dieser Technologien handeln. In der heutigen Zeit findet Wirtschaftskriminalität überwiegend aus der Ferne statt, also über IT- und Telekommunikationsverbindungen, insbesondere über das Internet. Alles deutet darauf hin, dass sich diese Tendenz in den kommenden Jahren verschärfen wird und es immer häufiger Cyberangriffe auf die schweizerischen Institute und digitalen Safes geben wird, auf die es alle abgesehen haben.

> *„Das Problem liegt in der Schere zwischen dem Gefahrenbewusstsein, den Risikoverwaltungsstrategien und den umgesetzten Cybersicherheitsmassnahmen.“*

Wie können die so gesammelten Daten verwendet werden?
Noch hinterhältiger ist, dass sich die Betrüger der Kommunikationswerkzeuge des Internets bedienen, um noch performanter zu werden. In sozialen Netzwerken und auf Datingservern können sich die Betrüger mit dem Opfer vertraut machen, es überwachen, Angriffe planen, Personen täuschen und sie so manipulieren (Social Engineering, Miss-

die **Cyperpiraten**

brauch von Zugriffsrechten, Installation von Schadprogrammen etc.), dass die Kriminellen in die betreffenden IT-Systeme eindringen, Transaktionen umleiten oder beispielsweise Überweisungen zu ihren Gunsten durchführen können.

Ferner ist auch die zunehmende Bedrohung durch Aktivisten und Terroristen nicht zu vernachlässigen. Diese übernehmen auf institutionellen Webseiten das Kommando und entstellen sie, hinterlassen Graffitis oder machen sie mit Denial-of-Service-Angriffen unzugänglich, um eine Ideologie zu verbreiten. Eine weitere ganz realistische und wenig in den Medien besprochene Bedrohung ist das Cryptolocking, bei dem IT-Ressourcen in eine Art Geiselhaft genommen und erst wieder freigegeben werden, wenn ein in Anbetracht der dadurch verursachten Probleme klein erscheinendes Lösegeld gezahlt wird (zwischen ein paar hundert und ein paar tausend Franken, häufig in virtuellem Geld wie z. B. Bitcoins zahlbar).

Können die Kosten dieser für die Banken immer besorgniserregenderen Cyberangriffe beziffert werden?
Da jede Situation und jeder Fall von Cyberkriminalität anders ist, können die direkten und indirekten Auswirkungen der Cyberrisiken sowie deren langfristige Dominoeffekte nicht beziffert bzw. korrekt bewertet werden. Die Wert-, Produktivitäts-, Vertrauens- und Imageverluste müssen also fallweise bewertet werden. Die Schäden für die betroffenen Organisationen und auch für deren Geschäftspartner und Kunden können allerdings sehr hoch sein. Und der Angriff auf eine bestimmte Organisation kann sich per Kettenreaktion oder Spiegeleffekt auf alle Organisationen des betroffenen Aktivitätssektors und damit beispielsweise auf den gesamten Finanzplatz eines Landes auswirken. Genau wie bei der klassischen Kriminalität trägt im Endeffekt die gesamte Gesellschaft die Kosten.

Sind sich die Banken über diese Gefahr ausreichend bewusst, und werden dort solide Strategien für die Verwaltung des digitalen Risikos umgesetzt?
Wie bewusst sich die Institute darüber sind und welche Gegenmassnahmen getroffen werden, hängt von der Kultur und den in der Vergangenheit gemachten Erfahrungen des jeweiligen Instituts ab. Wenn bereits Cyberrisiken aufgetreten sind, wird das Phänomen in der Regel besser eingeschätzt, und es ist dann auch klar, dass die Auswirkungen nicht rein virtueller Natur sind. In solchen Fällen ist es natürlich einfacher, die Geschäftsführung von der Sinnhaftigkeit einer Investition in Cybersicherheit zu überzeugen.

Das Problem liegt in der Schere zwischen dem Gefahrenbewusstsein, den Risikoverwaltungsstrategien und den umgesetzten Cybersicherheitsmassnahmen. Die Ausarbeitung der Sicherheitspolitik kann hinterherhinken, die Umsetzung ist möglicherweise nicht ausreichend, vorhandene Massnahmen werden eventuell umgangen, Prozesse nicht eingehalten, oder die Prüfprozesse sind nicht geeignet.

Wird es ein Verbot für den Zugriff auf die internen Systeme der Institute über Handys und sonstige persönlichen Geräte geben, um die Angriffsrisiken zu minimieren?
Durch die Informationstechnologien sind neue Risiken entstanden, die von den Instituten in ihrer Sicherheitspolitik unbe-

dingt berücksichtigt werden müssen. Die Schutzstrategien müssen realistisch sein und die heutigen Anforderungen wie insbesondere das mobile Arbeiten berücksichtigen, gleichzeitig aber auch ein geeignetes Sicherheitsniveau garantieren. Dabei handelt es sich häufig um Interessengegensätze. Um kohärent zu werden und ein gutes Gleichgewicht zu finden, muss ein Kompromiss gemacht werden. Es ist nicht vernünftig, ein hohes Sicherheitsniveau zu verlangen, gleichzeitig aber auch den Einsatz von Werkzeugen zu fordern, die keine robuste Sicherheit bieten, das Ganze dann noch kombiniert mit risikobehafteten menschlichen Verhaltensweisen. Auch beobachten wir eine Art technologische Flucht nach vorne, die teilweise durch das damit verbundene Prestige motiviert oder eine Folge von Einsparungsversuchen ist und die Institute und Kunden letztendlich gefährdet.

> *Les vulnérabilités inhérentes aux technologies, dont sont devenues dépendantes les institutions, les exposent en permanence à des cybermenaces.*

Die FINMA hat für den Datenschutz von Bankkunden neue Anforderungen gestellt. Sind diese für solche Bedrohungen ausreichend?
Regulatorische Zwänge vorzugeben und durchzusetzen, dass die Institute sich daran halten, ist häufig der erste Schritt zum verantwortlichen Handeln und zur Beachtung von Sicherheitsanforderungen. Die Vorschriften zu beachten ist allerdings nicht gleichbedeutend mit Betriebssicherheit. Eine der Gefahren besteht darin, Sicherheit mit Konformität zu verwechseln. Dies würde bedeuten, viele Ressourcen für die Konformität aufzuwenden anstatt für die Sicherheit und die strategische und betriebliche Kohärenz zur tatsächlichen Risikoentwicklung der Institute im Tagesgeschäft.

Wie können kleine Unternehmen, wie es die unabhängigen Vermögensverwalter häufig sind, das digitale Risiko in den Griff bekommen?
Die digitale Sicherheit ist so komplex und setzt so viele Kompetenzen voraus, dass kleine Unternehmen häufig überfordert sind. Daher ist es sehr wichtig für sie, sich auf Unternehmen stützen zu können, die einen integrierten «schlüsselfertigen» Service mit Lösungen sowohl für die technischen als auch für die verwalterischen, rechtlichen und menschlichen Aspekte bieten, und zwar im Vorhinein für den Schutz und die Verhinderung solcher Vorfälle sowie im Nachhinein für eine schnelle Reaktion und für die Krisenverwaltung. Nach dem Vorfall zu agieren ist nicht nur für die Schadensbegrenzung und -beseitigung fundamental wichtig, sondern auch um zu verstehen, was passiert ist, um die Ursachen und Verursacher zu identifizieren und um die notwendigen Massnahmen umzusetzen, damit es nicht noch einmal zu demselben Vorfall kommt. Bei solchen Massnahmen kann es sich um Schulungen oder um eine Begleitung bei Themen wie dem grundlegenden Umgang mit digitalen Daten, der globalen Sicherheitsstrategie inklusive der Cybersicherheit, der Abwehr von wirtschaftlicher Einmischung, der Installationssicherheit sowie der Sicherheitsanalysen handeln.

Wohin kann man sich wenden, wenn man sich schützen möchte?
Digitale Ermittlungen durchzuführen und digitale Protokolle zu identifizieren, zu finden, zu sammeln, aufzubewahren und zu interpretieren setzt echtes Know-how voraus. Unabhängig vom Ziel der digitalen Ermittlung – besserer Schutz für das Unternehmen, Erstattung einer Anzeige oder Begleitung der Rechts- und Polizeiinstanzen bei ihrer Arbeit – muss der auf forensische Informatik spezialisierte Ermittler nicht nur ganz spezifische technische Kompetenzen aufweisen, sondern seine Ergebnisse auch auf verständliche Art und Weise vor Nichttechnikern präsentieren können. Darüber hinaus ist die Unternehmensleitung sowohl in kleinen als auch in grossen Strukturen dem Risiko der Rufschädigung ausgesetzt, wenn ihre persönlichen Daten missbraucht oder gestohlen werden. Dies kann kompromittierend sein und dem Image der Organisation schaden. Sofern intern kein solches Know-how vorhanden ist, müssen sich die kleinen Unternehmen daher auch auf spezifische Kompetenzen stützen können, um Probleme rund um die Verwaltung und den Schutz ihres Onlinerufs zu behandeln. •

Cyberkriminalität in der Schweiz

26% der Schweizer Unternehmen sind 2014 zum Ziel von Cyberattacken geworden. Damit findet sich Cyberkriminalität nach der Unterschlagung auf dem zweiten Rang der am häufigsten angezeigten Wirtschaftskriminalität.

40% der Organisationen denken, dass sie in Zukunft zum Opfer von Cybercrime werden. Dieser Anteil ist höher als die Prognose für den Bereich Unterschlagung. Es ist bemerkenswert, dass 60% der Unternehmen davon ausgehen, dass sie nicht angegriffen werden!

23% der Befragten sind nicht in der Lage, die finanziellen Auswirkungen zu quantifizieren, die ihnen durch Cyberattacken entstanden sind. Diese Zahl belegt das wachsende Bewusstsein für die Gefahr, die die Cyberkriminalität in der Schweiz darstellt.

Quelle: PWC « Global Economic Crime Survey 2014, Economic Crime: A Swiss Perspective». Im Rahmen dieser repräsentativen Studie wurden Schweizer Unternehmen befragt. Über die Hälfte der Befragten sind aus der Finanzindustrie, im verarbeitenden Gewerbe sowie im Ingenieur- und Bauwesen.