Finanzintermediäre und digitales Aikido

Lektion V: Identifiziere deinen (Cyber-)Feind

In unseren vorhergehenden Artikeln ging es um den Umgang mit Mitbewerbern, Gegnern und Technologie durch die Umsetzung der Grundsätze des «digitalen Aikido». Wir möchten nun dieses Konzept der Selbstverteidigung wieder aufgreifen – denn wo könnte es wirksamer sein, als gegen die neue Angriffsform im Cyberspace?

Es ist hierbei besonders wichtig, den Feind genau zu identifizieren. Als erstes gilt es festzustellen, ob sich der Feind innerhalb oder ausserhalb Ihres Unternehmens befindet. Die Verteidigung gegen die Bedrohung von innen ist am schwierigsten, da Mitarbeiter umfassend und berechtigterweise Zugriff auf Ihre Vermögenswerte und Infrastruktur haben. Auch ist der Umgang mit dem internen Angriff besonders heikel, weil man seine Mitarbeiter nicht als Verdächtigte behandeln möchte. Es kann verschiedene mögliche Gründe für einen Angriff durch einen Mitarbeiter geben: menschliches Fehlverhalten, Unwissenheit, Unzufriedenheit über die Karriereentwicklung oder das Arbeitsumfeld und viele mehr. Mit technischen Massnahmen können diese Risiken zwar gemindert werden, aber das wichtigste und schwierigste Verteidigungsmittel ist die Wahrung einer gesunden Unternehmenskultur und die Kenntnis der eigenen Leute. Eine klare und transparente Kommunikation ist dabei von zentraler Bedeutung.

Externe Angreifer haben andere Absichten und lassen sich in drei weit gefasste Kategorien aufteilen:

1. Hacker: Hacker haben keine finanziellen Interessen, sondern eher das Bedürfnis, das Establishment zu bekämpfen. Oder sie wollen einfach ihr Ego aufpolieren, indem sie David gegen Goliath spielen.
2. Kriminelle: Normalerweise versuchen Cyberkriminelle, sich durch Datenverwendung / Identitätsdiebstahl oder Erpressung (z.B. über Distributed Denial of Service (DDoS) oder Datenverschlüsselung) oder Industriespionage einen finanziellen Nutzen zu verschaffen.
3. Terroristen: Terroristen verwenden ähnliche Techniken wie Hacker und Kriminelle, möchten aber Ländern, Unternehmen oder Personen Schaden zufügen.

Angriffsmuster
Durch die wachsende Vernetzung und die zunehmende Komplexität unserer weltweiten Infrastruktur entsteht ein Risiko der Verwundbarkeit, und auch die Risikovektoren haben sich verändert. Nachstehend ein paar typische Beispiele:

Identitätsdiebstahl	Zuerst wird ein Passwort geknackt, dann wird ein Profil (z.B. in den sozialen Medien) oder ein E-Mail-Account missbräuchlich verwendet, um eigene Mitteilungen (oder Viren / Trojaner) zu verschicken oder den Besitzer zu erpressen. Phishing ist eine dieser Techniken. Ein typisches Beispiel in unserer Branche ist der betrügerische Zahlungsauftrag.
Viren / Trojaner	Das Angriffsspektrum reicht von Spionage bis hin zur Absicht, die Daten und / oder die Infrastruktur infizierter Systeme zu zerstören oder einen Computer (unerlaubterweise) beispielsweise über ein Botnet zu verwenden.
Datendiebstahl	Hier verschafft man sich Zugriff auf ein System, um Daten zu stehlen. Diese werden dann entweder auf dem Schwarzmarkt verkauft oder verwendet, um der Öffentlichkeit Schaden zuzufügen oder um auf Kosten des Eigentümers Vorteile zu erlangen. Insbesondere im Finanzdienstleistungsgeschäft ist der Diebstahl von persönlichen Daten der Kunden eine äusserst schwerwiegende Bedrohung. Die finanzielle Situation jedes einzelnen Menschen ist sehr empfindlich und es muss alles unternommen werden, um sie vor kriminellem Missbrauch zu schützen.
DDoS	Bei einer «Distributed-Denial-of-Service»-Attacke wird durch den Versand einer grossen Anzahl von Anfragen an einen bestimmten Server ein Systemausfall herbeigeführt.
Naturkatastrophe	Stromausfall, Feuer, Flut, Erdbeben.

Schutz wertvoller Daten – für das Vertrauen der Kunden eine wichtige Voraussetzung
Wir müssen die Daten unserer Kunden und unserer Mitarbeiter schützen. Wir müssen ausserdem unsere Kunden und ihr Geschäft vor Betrug (z.B. falsche Zahlungen) schützen. Und wir müssen unsere Systeme schützen, damit diese operativ bleiben.

Die Techniken, die wir meistern müssen, sind so breit gefächert, dass wir in diesem Artikel bewusst nur einen Überblick geben. Für all diese Bedrohungen sollte Ihre Organisation über einen klaren BCM-Plan (Business Continuity Management) verfügen. Mit einem solchen Plan werden die Risiken identifiziert und priorisiert und dann Massnahmen zu deren Eindämmung umgesetzt. Typische Massnahmen sind der Besitz von redundanten IT-Systemen, die geografisch verteilt sind, Backup-Arbeitsplätze, die mit der gleichen Technologie ausgerüstet sind, sowie weitere Verfahrenselemente wie Kontaktlisten. Ein Empfehlungsbericht für das BCM ist auf der Website der Schweizerischen Bankiervereinigung (www.swissbanking.org) verfügbar. Unserer Erfahrung nach ist es gut, einen Plan zu haben. Aber es ist noch besser, wenn man diesen vorher getestet hat. Führen Sie bei Ihrem System einen Failover-Test durch, um zu sehen, was in der Praxis konkret abläuft – denn auf Papier überzeugt noch so mancher Plan …

Um festzustellen, wie solide Ihre Verteidigungsvorkehrungen sind, können Sie Ihrem (internen oder externen) IT-Anbieter zehn wichtige Fragen stellen:

1. Welche Schutzmassnahmen haben Sie gegen Viren, Trojaner und andere Arten von Malware und Spam?
2. Sind Firewalls installiert und welches sind die aktiven Regeln?
3. Falls Ihre Systeme nicht über ein Zwei-Faktor-Verfahren geschützt sind: Was ist der Grund dafür und welche Risiken bestehen?
4. Verfügen Sie über redundante Sicherungssysteme, und wann wurde bei Ihrem System das letzte Mal ein Failover-Test erfolgreich durchgeführt?
5. Stehen Ihnen im Falle eines Problems unabhängig betriebene Computer zur Verfügung?
6. Welche Log-Files sind vorhanden und wozu dienen sie?
7. Haben Sie eine Least-Privilege-Policy für den Datenzugriff, die klar definiert ist und entsprechend umgesetzt wird?
8. Wurde eine Software-Inventarisierung durchgeführt, in der Alter, letzte Aktualisierungen und andere wichtige Daten aufgeführt sind? Gibt es für intern entwickelte Software stets mindestens zwei Personen, die sich mit dem Code auskennen?
9. Welche zusätzliche Vorsorge und Massnahmen werden bei der Nutzung von Cloud-Diensten getroffen?
10. Wie wirksam sind Ihre Daten verschlüsselt?

BCM und IT-Sicherheit sind Aspekte, die nicht delegiert werden dürfen. Sie sollten regelmässig Ihre eigene Risikoeinschätzung vornehmen und Ihre Lieferanten und Dienstleister in diesen Prozess einbeziehen. Sorgen Sie dafür, dass dieses Thema fortlaufend ein wichtiges Anliegen bleibt.

Und zu guter Letzt – nachdem Sie sich um die Cyper-Risiken für Ihr Geschäft gekümmert haben, befassen Sie sich damit, wie Sie Ihren Kunden beim Schutz ihrer Privatsphäre helfen können. Insbesondere falls diese Kinder haben, die uneingeschränkt auf soziale Medien zugreifen. Mit diesem Thema werden wir uns in unserem nächsten Artikel über die sozialen Medien beschäftigen.

Sie können auch bestehende Checklisten zur Hilfe nehmen, wie diejenigen, die das Eidgenössische Finanzdepartment oder das Team für Online-Sicherheit von UBS veröffentlicht hat.

https://www.melani.admin.ch/melani/de/home.html
https://www.ubs.com/ch/en/online-services/security.html#tips

Matthias Plattner ist Head Technology & Processes bei UBS Global Financial Intermediaries. Wenn Sie Fragen zu diesem Thema und seiner Bedeutung für unsere Branche haben, wenden Sie sich bitte an: matthias.plattner@ubs.com.