www.pwc.de

Cyber-Kriminalität
Bedrohungen und Sicherheitsmaßnahmen in der Finanzindustrie

Im Zuge der Digitalisierung von Geschäftsprozessen stellt „Cyber-Kriminalität" eine ernsthafte Bedrohung für den Finanzdienstleistungssektor dar. Wir zeigen Ihnen anhand von Beispielen, wie Cyber-Kriminelle vorgehen und wie Sie sich gegen Angriffe schützen können.

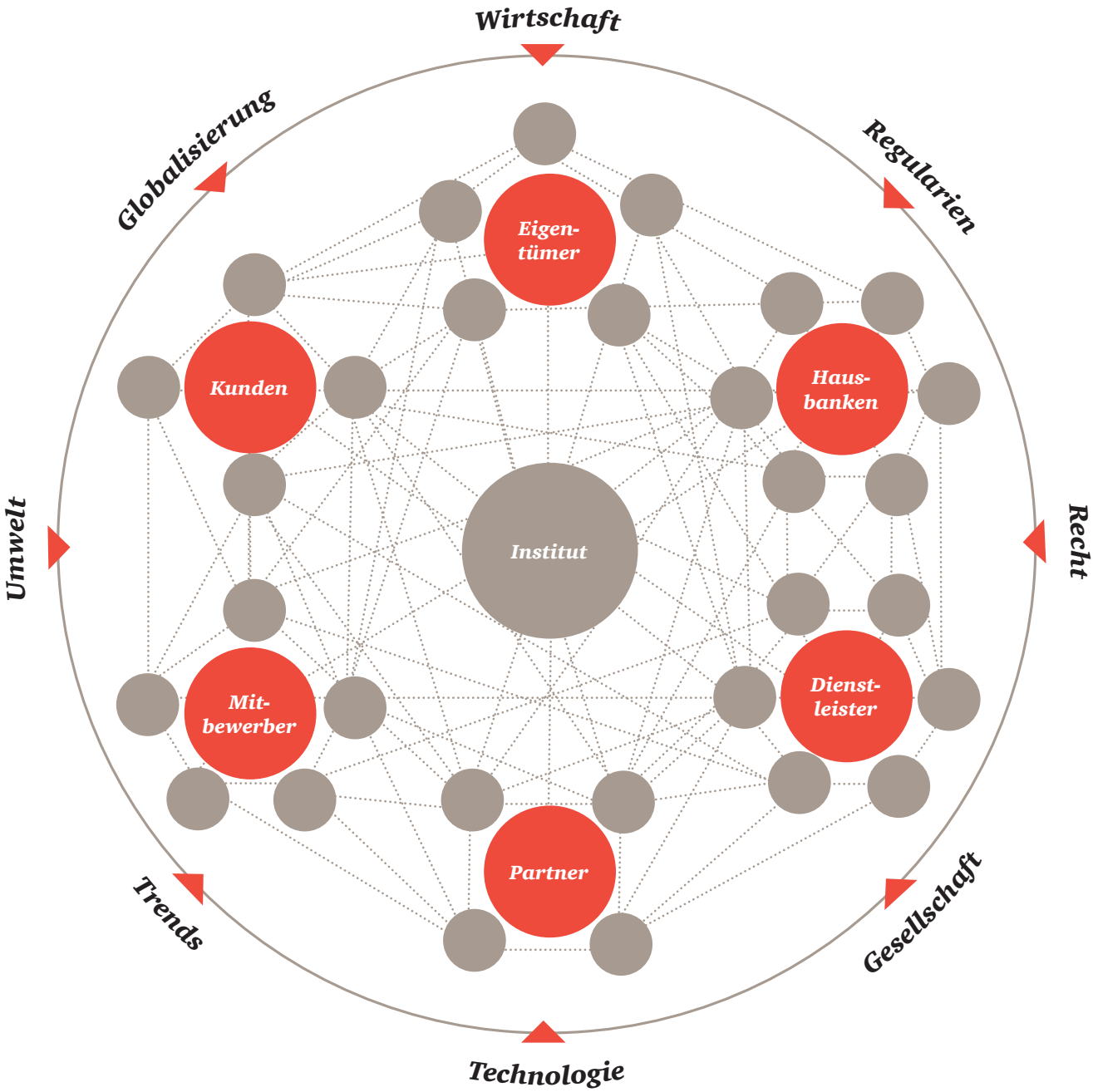
pwc

Neue Risiken im digitalen Ökosystem

Das digitale Ökosystem von Finanzinstituten wächst und verändert sich mit zunehmender Vernetzung mit Kunden, Dienstleistern, Hausbanken etc.

Dadurch ergeben sich die folgenden Risiken:

- Die Abhängigkeit von Technologie und digitalen Prozessketten erhöht sich.
- Transaktionen und Prozesse verteilen sich über das Ökosystem.
- Angreifer machen sich Lücken bei Geschäftspartnern zunehmend zunutze.
- Drittanbieter-Risiken rücken zunehmend in den Fokus der Aufsicht.



Cyber-Risiken – Beispiele aus der Praxis

Malicious E-Mail Attachment

Ein Mitarbeiter einer Versicherung erhält nach einem Anruf eines vermeintlichen Lieferanten eine Rechnung als E-Mail. Die angehängte PDF-Datei ist jedoch mit Schadcode infiziert. Ausgehend vom Endgerät des Mitarbeiters erhält der Angreifer durch Eskalation der Rechte Zugriff auf weitere Systeme. Mehrere Millionen Datensätze mit hochsensiblen Kundendaten werden kopiert und im Internet verkauft. Straf-zahlungen, Schadensersatz und Kosten für die Aufklärung kosten einen zweistelligen Millionenbetrag.

Malicious USB Stick

Vor der Zentrale eines Vermögensverwalters werden kostenlose USB-Sticks verteilt. Die Sticks sind mit einer bisher unbekannten Schadsoftware infiziert. Mehrere Mitarbeiter nutzen die Sticks im beruflichen Laptop. Die installierte Anti-Viren-Software erkennt keine Auffälligkeiten. Nach Übernahme der Kontrolle verändern die Angreifer eingehende Marktdateninformationen und veranlassen damit die Mitarbeiter zu Handels-entscheidungen zu ihren eigenen Gunsten.

Watering Hole

Die Log-in-Seite eines Hotels zu einem Internet-Hotspot, welche durch einen Mitarbeiter einer M&A-Beratung auf Dienstreise genutzt wird, ist mit einer Schadsoftware infiziert. Durch einen platzierten „Drive-by-Exploit“, durch den unbeabsichtigt Schadsoftware installiert wird, haben die Angreifer nach Aufruf der Seite vollen Zugriff auf die Geschäfts- und Kundendaten, das Mikrofon sowie die Kamera des M&A-Beraters. Sie sind über die M&A-Vorgänge bestens informiert und nutzen das Wissen für Insiderhandel.

Logic Bomb

Einem Administrator wurde gekündigt und dieser setzt vor dem Austritt aus der Bank seine privilegierten Berechtigungen ein, um eine Schadsoftware in den IT-Systemen der Bank zu verstecken. Aufgrund unzureichender Überwachung wird die „Zeitbombe“ nicht entdeckt und löscht zu einem bestimmten Zeitpunkt alle Kundendaten. Durch das mehrere Stunden dauernde Einspielen der Datensicherungen kommt der IT-Betrieb in dieser Zeit teilweise komplett zum Erliegen.

Spear Phishing

Bei einem IT-Dienstleister eines Asset-Managers erhält ein Mitarbeiter eine auf ihn persönlich angepasste, authentisch wirkende E-Mail, die ihn dazu auffordert, auf einer präparierten Seite seine Log-in-Daten einzugeben. Aufgrund einer fehlenden Zwei-Faktor-Authentifizierung genügen dem Angreifer diese Informationen, um sich Zugriff auf Anwendungen im Kundennetzwerk zu verschaffen. Der Angreifer verzögert minimal Orderaufträge und profitiert von gewinnbringenden Entwicklungen der Kurse.

Advanced Persistent Threat

Nach der initialen Infiltrierung des Banknetzwerks werden Systeme, Prozesse und Verhaltensweisen von Mitarbeitern über Monate hinweg beobachtet. Die Angreifer nutzen das gewonnene Wissen zur unauffälligen und unerkannten Manipulation der Buchhaltungssysteme, der automatischen Geldausgabe an Bankautomaten und zur Erhöhung der Kreditkartenlimite. Die Datensicherungen der letzten Monate sind infiziert und unbrauchbar. Große Teile der IT-Systeme müssen vollständig neu aufgesetzt werden.

Data Leakage

Die Mitglieder der Geschäftsführung einer Bank erhalten ein Tablet für den Zugriff auf die geschäftlichen E-Mails. Eine unzureichende Verschlüsselung des Datenverkehrs zwischen den Tablets und dem Banknetzwerk ermöglicht es Angreifern, Datenpakete auf einer Geschäftsreise im WLAN des Hotels abzugreifen und so an streng vertrauliche Daten zu gelangen. Die Angreifer bieten die vertraulichen Daten in Internetforen zum Verkauf an.

Malicious Patch

Ein kleiner Finanzdienstleister setzt für seine Handelsgeschäfte eine Fremdsoftware ein. In einem Expertenforum wird eine Schwachstelle in der Software verkündet und ein Security-Patch zum Download zur Verfügung gestellt. Der IT-Administrator installiert den Patch und bemerkt nicht, dass es sich bei diesem nicht um einen offiziellen Hersteller-Patch handelt. Eine in dem Patch enthaltene Schadsoftware wird installiert und sendet unbemerkt Kunden- und Firmendaten an den Angreifer.

Denial of Service

Eine Hackergruppe infiziert eine große Menge von Computern mit Schadsoftware und nutzt diese, um gleichzeitige Anfragen an die Internetserver einer großen Bank zu senden. Durch diese absichtlich herbeigeführte Überlastung der Server sind die Internetseiten der Bank nicht mehr verfügbar. Die Angreifer fordern von der Bank einen hohen Millionenbetrag für die Unterbindung der Attacke. Das Onlinebanking und weitere Dienste sind für die Kunden nicht nutzbar. Die Bank schafft es nur durch Umleiten des Datenverkehrs über einen spezialisierten Dienstleister, den Angriff abzuwehren.

Ransomware

Professionelle Hacker nutzen Sicherheitslücken in den IT-Systemen einer Leasing-gesellschaft aus, um zunächst unerkannt Ransomware auf den Systemen zu installieren. Mit deren Hilfe verhindern die Angreifer den Zugriff und die Nutzung des IT-Systems und verschlüsseln den gesamten Datenbestand auf den Windows-PCs. Die Angreifer fordern für die Freigabe und Entschlüsselung der Daten ein „Lösegeld“. Während der lang-wierigen Beseitigung der Schadsoftware können die Mitarbeiter nicht arbeiten und der Geschäftsbetrieb kommt zum Erliegen.

SQL-Injection

Beim Update des Onlinebankings einer großen Bank wurde aufgrund des Zeitdrucks für die neue Funktion kein Fokus auf die Sicherheit in der Softwareentwicklung gelegt. Angreifern ist es durch entstandene Lücken per SQL-Injection möglich, direkt Befehle in der Datenbank auszuführen und Kontrollen der Anwendung somit zu umgehen. Sie erhöhen Limits sowie Kontostände und führen Überweisungen unter anderen Konto-nummern durch. Die Überweisungen gehen auf Konten von Strohmännern und werden dort in Bitcoins umgewandelt.

Third-Party Risk

Eine Investmentgesellschaft hat große Teile ihrer IT-Systeme an einen Anbieter für Cloud Computing ausgelagert. Die Gesellschaft nutzt dabei die Datenbanksysteme des Cloud-Dienstleisters zur Verwaltung ihrer Geschäftsdaten. Durch unzureichende Zugriffsschutzmaßnahmen haben Administratoren des Dienstleisters unbeschränkt Einsicht in die Investitionen der Gesellschaft. Sie nutzen das Wissen über Investment-entscheidungen der Experten und tätigen eigene Investitionen zur persönlichen Bereicherung.

Schützen Sie sich vor den Angriffen von Cyber-Kriminellen

Übliches Vorgehen von Angreifern

Auskundschaften öffentlich zugänglicher Informationen

Angriff durch Watering Hole, Spear-Phishing-E-Mails etc.

Infizierung des ersten IT-Systems

Ausweitung der Berechtigungen und Analyse der Systeme

Ausweitung der Kontrolle in weiteren IT-Systemen

Sammlung und/oder Manipulation von Daten

Ausschleusung von Daten und Verwischen von Spuren

Notwendige Sicherheitsmaßnahmen

Identify
- Inventarisierung der Daten und Systeme
- Risikobewertung und Klassifizierung
- Security Governance

Protect
- Awareness-Maßnahmen und Schulungen
- Identity-&-Access-Management
- Data Leakage Prevention
- robuste Anwendungen und Systeme
- moderne Sicherheitssoftware

Detect
- Cyber-Intelligence
- Continuous Monitoring
- Anomalie- und Event-Management

Respond
- Analyse laufender Angriffe und Auswirkungsanalyse
- Incident Response
- Mitigationsfähigkeiten
- Krisenmanagement und -kommunikation

Recover
- Business-Continuity-Management
- Analyse erfolgreicher und abgewehrter Angriffe
- kontinuierliche Verbesserung

Ihre Herausforderungen

- Cyber-Risiken müssen erkannt und mit einem ganzheitlichen Blick auf die komplexe Thematik adressiert werden. Herkömmliche Sicherheitsmaßnahmen und -technologien reichen dafür nicht mehr aus.
- Cyber-Security stellt damit kein reines IT-Thema dar, sondern ist inzwischen eine geschäftliche Notwendigkeit in der Verantwortung des Top-Managements.

Ihre Ansprechpartner

Wenn Sie weitere Informationen wünschen, nehmen Sie gern Kontakt mit uns auf.

WP StB Marc Billeb
CISA
Tel.: +49 69 9585-2723
marc.billeb@de.pwc.com

Karsten Wilop
CISA, CGEIT, CRISC
Tel.: +49 211 981-1931
karsten.wilop@de.pwc.com

Achim Schäfer
CISA
Tel.: +49 69 9585-1022
achim.schaefer@de.pwc.com

Dr. Jens Vykoukal
CISA
Tel.: +49 69 9585-6992
jens.vykoukal@de.pwc.com

Unsere Expertise

PwC verfügt weltweit über mehr als 1.600 IT- und Cyber-Security-Experten, darunter mehr als 100 in Deutschland auf Financial Services spezialisierte Mitarbeiter. Unsere Experten haben langjährige Erfahrung in der Beratung und Prüfung von Cyber-Security-Organisationen sowie zu relevanten Schwerpunktthemen (zum Beispiel Informationssicherheitsmanagement, Identity and Access Management, SIEM oder Systemadministration). Mit unserer vielfach bewährten und herstellerunabhängigen Methodik sowie umfassenden Erfahrungen im Rahmen von Beratungsprojekten decken wir alle relevanten Themen im Bereich „Cyber-Security“ vollständig ab.

Zudem erfüllt unser risikoorientiertes Vorgehen durch die Berücksichtigung regulatorischer und gesetzlicher Vorgaben (unter anderem MaRisk, KWG und BDSG) sowie gängiger Standards (unter anderem ISO 2700x, BSI-Grundschutz, COBIT und ITIL) alle Compliance-Anforderungen in der Finanzindustrie. Sie profitieren dabei von unserem risikoorientierten und individuellen Ansatz, mit dem Sie ein wirksames und Compliance-konformes Cyber-Security-Programm umsetzen können. Zusätzlich realisieren Sie Einsparpotenziale bei anderen Prozessen sowie ein erhöhtes Maß an tatsächlicher Sicherheit.

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 157 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC. 9.400 engagierte Menschen an 29 Standorten. 1,55 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

www.pwc.de