# *Cyberrisiken in der Vermögensverwaltung*

# Mehr als nur ein Technologieaspekt

***Von Jan Schreuder***
*Leiter Cybersicherheit*
*PwC Schweiz*

Es gab in jüngster Zeit diverse Schlagzeilen über spektakuläre Cyberattacken auf grosse Organisationen. Dies vor allem in Ländern wie den Vereinigten Staaten, die über obligatorische Vorschriften bezüglich der Offenlegung von Datensicherheitsverletzungen verfügen. Diese Beispiele sind aber nur die Spitze des Eisbergs. In vielen Ländern in Europa, wie der Schweiz, gibt es noch keine obligatorische Offenlegungsanforderung für Datensicherheitsverletzungen, weshalb viele Attacken gar nicht erst publik gemacht werden. Ausserdem müssen Sicherheitsverletzungen auch in den Vereinigten Staaten nur gemeldet werden, falls Kundendaten betroffen sind – also zum Beispiel nicht im Falle eines Diebstahls von geistigem Eigentum.

**Welche Cyberrisiken bedrohen das Unternehmen?**

Um Cyberrisiken richtig einschätzen zu können, müssen die verschiedenen Typen von Bedrohungsakteuren sowie deren Motivation und Ziele verstanden werden. Wir beobachten momentan eine Art «Digitalisierung der Kriminalität». Klassischer Betrug wird dabei anhand von immer anspruchsvolleren Cyberattacken begangen. Die meisten Unternehmen sind sich der Gefahr, die von *organisierten Verbrechersyndikaten* ausgeht, durchaus bewusst. Wenn wir Cyberrisiken bewerten, gehen wir aber üblicherweise von drei weiteren Bedrohungsakteuren aus: Nationalstaaten, Hacktivisten und Insider.

Von *Nationalstaaten* finanzierte Cyberattacken werden von gut ausgerüsteten personellen Ressourcen mit hochentwickelten Fertigkeiten ausgeführt und zielen auf geistiges Eigentum sowie Informationen mit Wert für nationale Interessen ab. Das könnten politische, militärische, aber auch kommerzielle Interessen des Landes oder von Organisationen im Land sein. Angreifer, die im Auftrag von Nationalstaaten handeln, sind normalerweise «leise». Sie versuchen unter dem Radar zu bleiben, Informationen zu entwenden und so lange wie möglich unerkannt zu bleiben.

Ein anderer Bedrohungsakteur sind *Hacktivisten*-Gruppen, die mit Unternehmensaktivitäten auf einer ethischen, moralischen, politischen oder ideologischen Ebene nicht übereinstimmen. So gibt es zum Beispiel eine Vielzahl von Firmen, die von Hacktivisten angegriffen wurden, weil ihnen deren ökologische Praktiken oder Arbeitsbedingungen widersprachen. Hacktivisten tendieren dazu, «laut» zu sein. Sie wollen Störungen verursachen, um damit Aufmerksamkeit für ihre Sache zu erlangen.

Am schwierigsten ist Cyberattacken von *Insidern* entgegenzuwirken. Insider haben Zugriff auf sensitive Informationen oder die Möglichkeit, Transaktionen zu autorisieren und können ihre Zugriffsrechte entsprechend missbrauchen. In letzter Zeit gab es eine steigende Anzahl von Insidern, die zusammen mit externen Parteien Cyberverbrechen begangen haben. Das können Personen sein, die gezielt von kriminellen Organisationen in Unternehmen platziert werden, oder Personen, die schon lange im Unternehmen sind und von Kriminellen zur Kooperation erpresst werden.

**Was sind potenzielle Auswirkungen?**

Eine der bedeutendsten Auswirkungen von Cyberattacken können Reputationsschäden sein. Eine erfolgreiche Cyberattacke, die publik wird, hat fast immer eine bedeutende Auswirkung auf die Reputation eines Unternehmens. Entweder weil das Vertrauen der Kunden in die Kompetenz des Unternehmens, Informationen angemessen zu schützen, verloren geht oder weil interne Kommunikation und E-Mails, die potenziell unangenehme Informationen enthalten, an die Medien und damit an die Öffentlichkeit gelangen.

Die Reputation eines Unternehmens kann dabei auch durch das private Verhalten von Mitarbeitenden oder der Unternehmensführung, das überhaupt nichts mit der Geschäftstätigkeit zu tun hat, Schaden nehmen. Zum Beispiel durch eine Cyberattacke, die zur Offenlegung von Namen und E-Mail-Adressen von Mitarbeitenden eines Unternehmens, die auf einem Seitensprung-Portal angemeldet sind, führt.

**Cyberrisiken in der Vermögensverwaltung – Anlagebetrug**

Cyberattacken können auch wesentliche Auswirkungen auf die Aktienpreise von börsennotierten Unternehmen haben. Die Cyberrisiken im Investment-Portfolio von Unternehmen sind schwierig einzuschätzen. Die US-amerikanische Securities and Exchange Commission (SEC) verlangt zwar von Firmen, solche Risiken sowie entsprechende Kontrollen offenzulegen. Dies trifft aber auf die Mehrheit der anderen Sicherheitsregulatoren nicht zu. Investoren beginnen vermehrt damit, der Unternehmensführung Fragen zu ihren Cyberrisiken zu stellen. Die Kommunikation dieser Risiken an die Investoren ist jedoch noch längst nicht ausgereift.

Fälle von Anlagebetrug mithilfe von Cyberattacken haben stark zugenommen. In einem bekannten Fall in den USA werden Kriminelle verdächtigt, russische Hacker angeworben zu haben, um Kundenlisten und Informationen von grossen Finanzinstituten zu stehlen. Diese wurden dann für die Ausführung von traditionellen «Pump and Dump»- oder «Front Running»-Schemen missbraucht. Die Betrüger waren äusserst erfolgreich aufgrund der umfangreichen Informationen, die sie über die Investoren, deren Berater, ihre bisherigen Investments und deren Portfolio gesammelt hatten.

Kundenlisten und -informationen zu stehlen und sie für kriminelle Zwecke zu missbrauchen, ist nur *eine* Taktik von Cyberkriminellen. Jeder Broker und Portfoliomanager kennt das Risiko von Insiderhandel und besitzt entsprechende Überwachungssysteme im Betrieb, um sich dagegen zu schützen. Werden Insiderinformationen allerdings mittels einer Cyberattacke gestohlen, so ist es wesentlich schwieriger, dies herauszufinden.

**Diebstahl von geistigem Eigentum**

Der Wert vieler Unternehmen in diversen Industrien besteht zu einem grossen Teil aus geistigem Eigentum. Entweder in der Form von Patenten, Technologien, Software, Betriebsmodellen oder gar kommerziellen Abmachungen mit Schlüsselkunden und Lieferanten. Der Wert dieses geistigen Eigentums kann – oft über Nacht – stark beeinträchtigt werden, wenn ein Konkurrent oder eine andere interessierte Partei Zugriff auf diese Informationen erhält und sie ausnützt. Bei der Beurteilung des Werts von Investments sollten deshalb die Abhängigkeit von geistigem Eigentum und die Schutzmassnahmen für Letzteres sorgfältig berücksichtigt werden, speziell im Fall von Investments in Start-ups.

**Konsolidierungsrisiken bei Netzwerken und Datenzentren**

Viele Holdinggesellschaften verfolgen eine «Kaufen-konsolidieren-verkaufen»-Strategie, bei der Operationen in einem gemeinsamen Datenzentrum, Netzwerk oder Cloud-Service verschmolzen werden, um die Kosten zu reduzieren und Synergien zu nutzen. In diesem Prozess könnte versehentlich ein bereits infiziertes Netzwerk mit einem bisher sicheren Netzwerk verbunden werden. Damit bekämen Angreifer Zugriff auf ein grösseres Netzwerk, wovon eventuell die ganze Gruppe betroffen wäre. Auch wenn Firewalls und Netzwerksegregation eingesetzt werden, ist es schwierig, hochentwickelte Angreifer im Netzwerk zu erkennen und die Attacken einzudämmen. Ähnliche Risiken entstehen, wenn Gruppen getrennt und verkauft werden.

**Zahlungsbetrug**

Eine übliche Cyberattacke ist es, sich Zugriff zu E-Mail-Konten oder anderen persönlichen Daten von Führungskräften zu verschaffen, um damit Finanzangestellte dazu zu bewegen, falsche Zahlungen zu initiieren und durchzuführen. In Fällen, die wir in der Schweiz beobachtet haben, nutzten Angreifer streng geheime Informationen über die Unternehmen und deren Operationen, um Glaubwürdigkeit herzustellen. Sie setzten eine Kombination von Telefongesprächen und E-Mails ein, scheinbar von Führungskräften ausgehend, um den Betrug durchzuführen. Mithilfe des Zugriffs auf die E-Mail-Posteingänge der Führungskräfte bestätigten die Betrüger ihre versandten Anweisungen gleich selbst, wenn die Finanzangestellten um die Freigabe baten.

**Marktmanipulation**

Es gibt eine Reihe von bekannten Beispielen für Marktmanipulationsversuche. Zum Beispiel als die «Associated Press» scheinbar twitterte, dass das Weisse Haus gerade bombardiert worden war und innerhalb von Minuten über 136 Mrd. US$ auf den globalen Märkten abgeschrieben werden mussten. Solche viel beachteten Manipulationen werden zwar schnell identifiziert und innerhalb von wenigen Minuten korrigiert. Es gibt aber auch subtilere Attacken, die viel länger unerkannt bleiben und signifikante Auswirkungen haben können. Trading-Teams müssen sich bewusst sein, dass Märkte durch die Verbreitung von falschen Informationen potenziell manipuliert werden, auch wenn die Quelle als vertrauenswürdig erscheint.

Das Bewusstsein für und die Übersicht über Cyberrisiken sollten nicht nur einer kleinen Gruppe von Leuten im Unternehmen vorbehalten sein. Mitarbeitende, die sich in der Position befinden, potenzielle Cyberattacken zu erkennen und entsprechend zu handeln, müssen ebenfalls mit eingebunden werden – zum Beispiel das Zahlungsteam, die Portfoliomanager oder das Trading Desk.

**Wie mit Cyberrisiken umgehen?**

Cyberrisiken können viele verschiedene Bereiche einer Organisation beeinflussen. Die genannten Beispiele zeigen, dass der Umgang mit diesen Risiken nicht nur als Technologieaspekt behandelt werden sollte, der den IT-Verantwortlichen überlassen wird. Vielmehr muss auch die Geschäftsleitung ein gutes Verständnis von den Cyberrisiken haben, die ihre Organisation bedrohen, und wissen, wie sie diesen begegnen kann.

Ein Schutz gegenüber Cyberrisiken beginnt mit *situativem Bewusstsein* – einer guten Übersicht über die verschiedenen Typen von Cyberattacken, die auf andere Unternehmen zielen und einen Einfluss auf das eigene Unternehmen haben könnten, sowie einer klaren Einsicht in die eigenen Schlüsselinformationen und die bedrohten Bereiche des Unternehmens. In sogenannte «Threat Intelligence» zu investieren und an «Threat Intelligence»-Foren teilzunehmen, kann hier einen wesentlichen Beitrag leisten.

Das Bewusstsein für und die Übersicht über Cyberrisiken sollten nicht nur einer kleinen Gruppe von Leuten im Unternehmen vorbehalten sein. Mitarbeitende, die sich in der Position befinden, potenzielle Cyberattacken zu erkennen und entsprechend zu handeln, müssen ebenfalls mit eingebunden werden – z.B. das Zahlungsteam, die Portfoliomanager oder das Trading Desk.

***jan.schreuder@ch.pwc.com***
***www.pwc.ch***