«Die Zeit der Ausreden ist vorbei»

Matthias Bossardt, Leiter Cybersicherheit beim Wirtschaftsprüfungs- und Beratungsunternehmen KPMG, spricht im Interview über die Bedrohungslage in der Schweiz und darüber, wie Unternehmen sich schützen können.

KPMG

Matthias Bossardt, Leiter Cybersicherheit bei KPMG

Herr Bossardt, wie gross ist die Bedrohung durch Cyberkriminalität für die Menschen und Unternehmen und Menschen in der Schweiz?
Quantitativ ist das schwer abzuschätzen. Es gibt bisher keine belastbare Datenbasis zu Cybervorfällen in der Schweiz. Auch kann man in den bekannten Fällen die entstandenen Schäden nur sehr schwer zuverlässig beziffern. Dennoch: Die Gefahr wird klar grösser. Das erkennt man, wenn man die Bedrohungslage analysiert und sich die bekannten Fälle anschaut. Zum einen werden die Angreifer immer professioneller. Zum anderen vergrössert sich die Angriffsfläche mit dem Voranschreiten der Digitalisierung. Unsere Abhängigkeit von der vernetzten technischen Infrastruktur wächst – und damit auch die Bedrohung.

Mit welcher Art von Cyberkriminalität werden Sie bei Ihrer Arbeit konfrontiert?
Eine grosse Rolle spielen derzeit Angriffe mit Ransomware. Das sind Schadprogramme, welche die Daten auf dem Computer des Opfers verschlüsseln oder den Zugriff verhindern. Der Angreifer erpresst dann ein Lösegeld für die Freigabe. So ein Angriff kann jeden treffen, denn die Attacken erfolgen meistens nicht gezielt. Und sie können für die betroffenen Unternehmen einen grossen Schaden verursachen, das kann ans Überleben gehen. Angriffe mit Ransomware werden aus meiner Sicht stark unterschätzt. Die sogenannten Distributed-Denial-of-Service-Attacken, bei denen das Computersystem des Opfers überlastet wird, spielen dagegen heute keine grosse Rolle mehr. Derzeit kommt auch der sogenannte CEO-Fraud häufig vor: Mit gefälschten oder manipulierten E-Mails im Namen eines Managers erwirken Betrüger dabei eine Zahlung auf ihr Konto. Diese Methode wird systematisch angewendet – leider mit Erfolg und oftmals hohen Schadenssummen.
Neben diesen Angriffen von Kriminellen, die einfach Geld wollen, gibt es noch eine zweite Art von Vorfällen. Da geht es um Spionage oder um die Vorbereitung zu Sabotage. Diese Angriffe kommen häufig aus einem staatsnahen Umfeld und sind für die Opfer sehr schwer zu entdecken. Da muss man schon sehr genau hinschauen. Aber immer mehr Unternehmen schauen genau hin. Deshalb wissen wir, dass diese Dinge passieren – auch in der Schweiz.

Weiss man, wer hinter solchen Spionageattacken steckt?
Eigentlich hat man schon ein gutes Verständnis dafür, woher solche Angriffe kommen. Man untersucht die Malware und betreibt Reverse-Engineering. Die Art der vorhandenen Code-Fragmente lässt dann Schlüsse auf die Herkunft der Angreifer zu. Aber es ist politisch oft heikel, mit dem Finger auf andere zu zeigen, zumal Angreifer bewusst falsche Fährten legen können.

Wie gut sind die Schweizer Unternehmen inzwischen aufgestellt, um sich zu verteidigen?
In der Schweiz ist die Cyberhygiene besser als in anderen Ländern. Hier ist beispielsweise nur wenig Piratensoftware im Einsatz, und

KPMG bietet Hochschulen kostenlosen Zutritt zur digitalen Cyberakademie
Gemeinsam mit der britischen Cybersicherheitsfirma Immersive Labs hat KPMG Schweiz im vergangenen Herbst die Digital Cyber Academy (DCA) lanciert. Mit der innovativen Kooperation bietet KPMG sämtlichen Schweizer Hoch- und Fachhochschulen eine cloudbasierte Cybertrainings- und Bewertungsplattform kostenlos an. KPMG nutzt diese Plattform auch intern als Trainingsinstrument für die eigenen Cyberspezialisten.
Die Nutzer tauchen in der DCA in virtuelle Cyberlabore ein und werden in verschiedenen realen Fallbeispielen herausgefordert. Ziel ist es, die eigenen Kompetenzen im Umgang mit Cyberrisiken zielgerichtet weiterzuentwickeln und sich einen wichtigen Grundstein für die berufliche Zukunft im Cyberbereich zu legen. 365 Hoch- und Fachhochschulen in Australien, Grossbritannien, Kanada, Singapur und den USA nutzen laut KPMG die Plattform bereits, um die Fähigkeiten ihrer Studierenden in der Cybersicherheit und -abwehr kontinuierlich zu verbessern, und ihnen attraktive Karriereperspektiven zu ermöglichen.

die Software wird eher auf dem aktuellen Stand gehalten. Das hilft – zum Beispiel, wenn Ransomware-Wellen auftreten. Dennoch sind viele Unternehmen immer noch sehr einfach anzugreifen. Das zeigen auch unsere eigenen Tests. Bei vielen herrscht immer noch das Gefühl, dass es einen selbst nicht betrifft. Weil das Risiko nicht so greifbar ist, zögern viele, auch nur schon die Grundmassnahmen gezielt und systematisch umzusetzen.

«Unsere Abhängigkeit von der vernetzten technischen Infrastruktur wächst – und damit auch die Bedrohung.»

Welche grundlegenden Massnahmen sollte ein Unternehmen denn umsetzen, um sich hinreichend zu schützen?
Erst einmal ist es wichtig, dass die Unternehmen nicht nach dem Giesskannenprinzip vorgehen und dass sie nicht Massnahmen ergreifen, nur um formellen Anforderungen oder bestimmten Normen gerecht zu werden. Das bringt nichts. Man muss auch nicht Hunderte von Massnahmen umsetzen, sondern sich auf das konzentrieren, was wirklich wichtig ist: Sie müssen die Verantwortlichkeiten definieren, und Sie müssen wissen, was in Ihrem Unternehmen an technischen Systemen vorhanden ist. Sie müssen die Frage klären, was genau Sie eigentlich schützen wollen. Schulung der Mitarbeiter und das Problembewusstsein im Unternehmen sind ebenso von Bedeutung. Dann müssen vorbeugende Massnahmen, wie Identitäts- und Zugriffsmanagement, Aktualisieren der Systeme, Anti-Malware-Software und Netzsegmentierung umgesetzt werden. Und schliesslich muss ich in der Lage sein, einen Angriff zu entdecken, und ich brauche einen Plan, wie ich in solchen Fällen vorgehe. So einen Plan gibt es in vielen Firmen nicht. Und wenn es ihn gibt, haben die Mitarbeiter oft Hemmungen zu üben und einen Ernstfall mal durchzuspielen. Dabei könnte man ja schlecht aussehen. Aber wer ein guter Fussballspieler werden will, muss auch trainieren und dabei ein paarmal neben das Tor schiessen. All dies müssen sie übrigens auch von ihren Lieferanten, Dienstleistern und Geschäftspartnern einfordern, um sich nicht über «vertrauenswürdige» Dritte angreifbar zu machen.

Technische Massnahmen sind das eine. Aber ist das grösste Risiko am Ende nicht doch der Mensch?
Der Mensch ist sehr wichtig. Aber mit der Aussage, das grösste Risiko sei der Mensch, macht man es sich viel zu einfach. Das ist oft eine Ausrede dafür, nichts zu tun. Eine wirkungsvolle Cyberstrategie bezieht den Faktor Mensch mit ein und geht zum Beispiel davon aus, dass der Eine oder Andere auch mal eine Phishing-E-Mail anklickt. Ich würde es für

mich selbst auch nicht ausschliessen, dass ich auf eine gezielte Phishing-E-Mail hereinfallen würde. Hacker können auch eine an sich vertrauenswürdige Webseite angreifen und dort eine Schadsoftware einbetten, die dann alle Besucher dieser Seite infiziert. Man kann nicht erwarten, dass ein Nutzer so etwas erkennt. Das kann kein Mensch. Wenn solche Dinge passieren, sollte das betroffene Unternehmen dann nicht in seiner Existenz gefährdet werden. Deshalb muss man es dem Angreifer möglichst schwer machen, Schaden anzurichten. Wenn Ihr Eingangstor schon so schwach ist, dass Sie sagen: «Es soll keiner auf verdächtige Links klicken», wird das nie funktionieren.

100-prozentigen Schutz wird es wie bei allen Risiken auch bei der Computersicherheit nie geben. Wie viel Schutz ist sinnvoll und wirtschaftlich?

Das ist eine Frage, die ein Unternehmen individuell für sich entscheiden muss. Bisher hat man als Messgrösse den Anteil des IT-Budgets herangezogen, der für IT-Sicherheit ausgegeben wurde. Aber das ist kein gutes Mass. Das Cyber-Risiko ist ein operationelles Unternehmensrisiko. Die Höhe der IT-Ausgaben sagt nur wenig darüber aus, wie viel Sie in die Cybersicherheit investieren sollten. Man sollte da anders herangehen: Über die grundlegenden Hygienemassnahmen sollte man nicht diskutieren, die müssen flächendeckend umgesetzt werden und sind ganz einfach Teil der operativen Kosten. Darüber hinaus ist es wichtig, in Szenarien zu denken und sich zu fragen «Was sind die Dinge, die uns wirklich wehtun?» Das kann zum Beispiel so eine Ransomware-Attacke sein. Es sind Fälle von Grossunternehmen öffentlich bekannt, die Hunderte von Millionen Dollar an Schäden verursacht haben. Und bei einem kleinen Unternehmen kann das genauso kritisch sein. Man muss sich fragen: «Welche Massnahmen haben wir, um das zu verhindern? Und wenn diese Massnahmen nicht greifen – überleben wir das? Haben wir Vorkehrungen getroffen, um – wenn auch für eine gewisse Zeit eingeschränkt –weiterarbeiten zu können?»

Können sich auch kleine Unternehmen mit einer Handvoll Mitarbeitern effektiv schützen?

Alle können sich schützen. Die Grundmassnahmen kann auch ein Kleinbetrieb mit vier oder fünf Mitarbeitern umsetzen. Dabei ist es aber notwendig, sich genau zu überlegen, was man selbst macht. Wollen sie tatsächlich die IT selber betreiben? Den Strom generieren sie ja auch nicht mehr im eigenen Kraftwerk. Wenn sie auf einen professionellen IT-Dienstleister oder Cloudanbieter setzen, kann man ein hohes Sicherheitsniveau erreichen, ohne dass einem die Kosten um die Ohren fliegen. So oder so muss man ein Verständnis für die eigenen Risiken haben und für die Assets, die es zu schützen gilt. Und man muss die Strategie verstehen, mit der diese geschützt werden sollen.

Haben wir in der Schweiz genügend Spezialisten für Cybersicherheit?

Weltweit hat derzeit niemand genügend Spezialisten. Das muss man systematisch angehen. In der Schweiz gibt es verschiedene Initiativen, an Universitäten und Fachhochschulen, und auch die Armee hat jetzt einen Lehrgang für Cybersicherheit. Auch KPMG leistet mit der digitalen Cyberakademie [siehe Kasten] einen Beitrag dazu. Ich glaube auch, dass es genügend Interesse an dem Beruf gibt: Rolle und Ansehen der Sicherheitsexperten werden immer weiter aufgewertet. Heute muss ein solcher Experte umfassendes technisches Know-how haben. Gleichzeitig muss er in der Lage sein, die Cyberrisiken im Unternehmenskontext zu verstehen und der Geschäftsführung oder dem Verwaltungsrat zu berichten. Das macht den Job anspruchsvoll und spannend.

Für Sicherheit zu sorgen, ist nicht zuletzt auch Staatsaufgabe. Welche Rolle spielt der Staat bei der Cybersicherheit?

Die Aussage stimmt nur bedingt: Auch in der realen Welt muss ich mein Haus immer noch selbst abschliessen. In der virtuellen Welt ist das noch einmal komplizierter, denn dort gibt es keine Territorien. Zudem gehören die IT-Infrastrukturen privaten Unternehmen. Der Staat spielt eine Rolle beim Schutz unserer kritischen Infrastrukturen. Wenn beispielsweise jemand unsere Energieversorgung abschalten kann, dann betrifft das uns alle. In England hat Ransomware Spitäler lahmgelegt, und Operationen konnten nicht stattfinden. Das sind Beispiele, bei denen es um das Gemeinwohl geht, da spielt der Staat durchaus eine Rolle. Zudem ist die Strafverfolgung Sache des Staates.

Die Frage stellt sich, ob der Staat gerade auch im Zusammenhang mit vernetzten Geräten (Internet of Things) minimale Sicherheitsanforderungen vorgeben muss, damit wir hier nicht in ein Riesenproblem hineinlaufen. Aber der Staat kann und soll nicht die Unternehmen von ihrer Verantwortung in Sachen Sicherheit entbinden und sie vor Angriffen und deren Auswirkungen umfassend schützen. Noch einmal: Die Zeit der Ausreden ist vorbei. Es ist grobfahrlässig, wenn Unternehmen das Thema nicht ernsthaft angehen. Die Risiken sind real, es kann ans Eingemachte gehen. Wenn einen eine Ransomware unvorbereitet trifft, kann es sein, dass man sein Geschäft danach nicht mehr hat. Cybersicherheit ist heute Teil des Geschäfts – genau wie man einen Zaun um seine Produktionsanlagen macht. ●

«Mit der Aussage, das grösste Risiko sei der Mensch, macht man es sich viel zu einfach. Eine wirkungsvolle Cyberstrategie bezieht den Faktor Mensch mit ein.»

Interview:
Hendrik Thielemann

Zur Person: Matthias Bossardt

Dr. Matthias Bossardt ist Leiter Cyber Security, Datenschutz und Technology Risk Dienstleistungen bei KPMG Schweiz. Er arbeitet weltweit mit Organisationen aus verschiedenen Sektoren – insbesondere Finanzdienstleistern, Pharmaunternehmen sowie Technologie- und Telekommunikationsanbietern – zusammen und unterstützt sie beim Management von Cyber-, Informationssicherheits-, Datenschutz- und Technologierisiken. Im Oktober 2016 wählte die Wirtschaftszeitschrift Bilanz Bossardt zu einem der einflussreichsten «Digital Shapers» der Schweiz. Vor seinem Eintritt bei KPMG forschte Bossardt über Kommunikationssysteme und Cybersicherheit an der ETH Zürich und am Forschungsinstitut des Beckman Institute of Advanced Studies der University of Illinois, Urbana-Champaign. Er begann seine berufliche Karriere als Mikrochip-Ingenieur im Jahr 1998.