Grant Thornton

An instinct for growth™

Cyber-Sicherheit

Beratung

Risiko

Den Wert von Daten sichern

Ein Wechsel der Prioritäten im Risikomanagement

2017

Inhalt

Kurzfassung

Cyberrisiko auf den Punkt gebracht

Führungskräfte sehen sich heutzutage mit einer Reihe komplexer, miteinander verbundener und sich schnell weiterentwickelnder Risiken konfrontiert. Einer der kritischsten und am wenigsten verstandenen Risiken ist der Cyberangriff.

Eine der größten Herausforderungen stellt die virtuelle Natur der Bedrohung dar. Daten sind weit entfernt von der traditionellen Hardware oder Produkten, die genau definiert sind und durch übliche Unternehmensversicherungen versichert werden können. Allzu oft wird das Potenzial für einen Cyberangriff als IT-Problem und nicht als unternehmensweites Problem gesehen. Dennoch kann eine ernsthafte Sicherheitsverletzung katastrophalen Schaden verursachen: Das Vertrauen der Kunden wird untergraben, aufsichtsrechtliche Überprüfungen werden veranlasst, der Betrieb wird gestört und langfristige finanzielle Schäden werden verursacht.

Bei unserer Untersuchung verfolgten wir folgende Fragestellung: Wie können Führungskräfte heutzutage sicherstellen, dass die Cyberrisiken ihres Unternehmens bekannt und ausreichend adressiert sind?

Wir wollten über den Jargon, die technische Sprache und Schauermärchen der Medien hinausgehen, um einen praktischen Ansatz für heutige Führungskräfte zu erarbeiten, damit die Bedrohung des Cyberangriffs leichter bewältigt werden kann. Insbesondere wollten wir uns mit dem Risiko für Daten beschäftigen, denn letztendlich sind Daten jene Werte, die Unternehmen vor Hackern bzw. Angreifern schützen möchten.

„Unserer Ansicht nach ist ein effektives Cyberrisikomanagement nur möglich, wenn Unternehmen einen klaren Überblick über ihre Daten haben“, so Paul Jacobs, weltweiter Leiter des Bereiches Cyber-Sicherheit bei Grant Thornton. „Dies könnten E-Mail-Daten, Finanzinformationen, Kundendatensätze, geschützte Verfahren oder Geschäftsgeheimnisse sein. Erst wenn Unternehmen die Wichtigkeit dieser Daten vollständig verstehen und sie wissen, wo diese gespeichert sind – was in einigen Kreisen als Kategorisierung oder Klassifikation bekannt ist – können sie sichere Verteidigungsstrategien gegen Hacker implementieren – und zwar dort, wo sie am meisten gebraucht werden.“

Um den Reifegrad in diesem Bereich zu verstehen, haben wir 2.900 Führungskräfte für den International Business Report (IBR)[1] von Grant Thornton befragt. Darüber hinaus befragten wir 12 Personen, die aus dem Grant Thornton Netzwerk sowie aus Wissenschaft und Wirtschaft stammen und über Fachwissen im Bereich Cybersicherheit und Informationsmanagement verfügen.

„Die meisten Unternehmen sind der Meinung, dass bei ihnen nicht mit einer Datenschutzverletzung (Data Breach) zu rechnen ist. Ungefähr 20 % glauben, dass sie bald angegriffen werden und haben daher in ausgefeilte Cybersicherheitssysteme investiert, um sich darauf vorzubereiten. Ungefähr 30 % sind wahrscheinlich recht gut vorbereitet. Der Rest befindet sich im Durchschnitt oder glaubt nie Ziel solcher Cyberattacken zu werden.“

John Kan, Chief Information Officer, A*STAR (Agency for Science, Technology and Research)

1. Grant Thornton Umfrage im Q4 2016. Gesamte Methodologie am Ende dieses Berichts

Zentrale Erkenntnisse

Was Unternehmen im Zusammenhang mit ihren kritischen Daten wissen, sagen und tun

Vielen Unternehmen fehlt das Wissen über die Daten in ihrem Besitz.
Unternehmen erzeugen jeden Tag eine unglaubliche Menge an Daten. Der einfachste und billigste Weg, um all diese Informationen zu speichern, ist das „Deponie-Modell“, dessen Konzept darin besteht, alles zu behalten und so viel wie möglich in die Cloud zu verschieben. Wir sehen oft Fälle, in denen so verfahren wird, ohne auch nur den Versuch zu unternehmen, die enthaltenen Daten aufzuzeichnen. Unsere Umfrageergebnisse zeigen, dass nicht einmal zwei Drittel der Unternehmen (65 %) Maßnahmen ergreifen, um ihre Daten zu verstehen. Sie wissen weitgehend nicht, wie viele Daten sie besitzen, was diese Daten tun und welchen Schaden deren Kompromittierung verursachen könnte. Doch wenn sie diese Grundlagen nicht kennen, wie können sie dann sicher sein, dass sie die Daten richtig verwalten?

In den meisten Fällen weist das Risikomanagement ein datenförmiges Loch auf.
Mehr als ein Drittel aller Unternehmen (36 %) weist ihren Daten kein Risikoprofil zu. Das ist überraschend, wenn man bedenkt, was im Falle einer Datenschutzverletzung auf dem Spiel steht. Das mag eventuell daran liegen, dass die Führungsebene, obwohl sie akzeptiert, dass Cybersicherheit ein Risiko darstellt, immer noch nicht die erforderlichen Maßnahmen zur direkten Unterstützung von Entschärfungsmaßnahmen ergreift. Eine weitere Erklärung ist, dass der risikoseitige Fokus bisher weitgehend auf einer begrenzten Anzahl von Geschäftsrisiken lag, die versichert werden konnten. Infolgedessen haben ältere Risikoteams weniger Erfahrung in der Vorhersage, Verwaltung und Bewertung von virtuellen Bedrohungen wie Datenschutzverletzungen. Das muss sich ändern.

Viele Unternehmen „schützen alles und schützen dabei nichts“.
Über drei Viertel der Unternehmen (78 %) bauen eine allgemeine Cyberschutzmauer auf, ohne spezifische Maßnahmen zum Schutz ihrer wertvollsten Daten zu ergreifen. Im schlimmsten Fall bedeutet dies, dass sie teure Firewalls implementieren, die Daten von geringem Wert schützen, während die wichtigsten Informationen – nämlich diejenigen, die für Kernfunktionen der Unternehmen notwendig sind – exponierter sind als sie sein sollten.

30%
sind wahrscheinlich recht gut vorbereitet

50%
sind durchschnittlich gut vorbereitet oder glauben, dass sie nie Ziel solcher Cyberattacken werden

20%
glauben, dass sie bald ange-griffen werden und haben daher in ausgefeilte IT Security Systeme investiert, um sich entsprechend vorzubereiten

Um die Datenproblematik zu begreifen, muss man in alle Richtungen denken.
Für die meisten Unternehmen wäre es unmöglich, alle Kalkulationstabellen, archivierten E-Mails und erstellten Dateien zu bewerten und zu ordnen. Dieser Prozess kann auch nicht vollständig automatisiert werden: Das Verständnis von Risiko und Wert der Daten erfordert menschliches Urteilsvermögen.

Der richtige Umgang damit erfordert auch Vorstellungsvermögen. Man muss in der Lage zu sein wie ein zynischer und opportunistischer Hacker zu denken und Daten zu identifizieren, deren Kompromittierung und Verfälschung den Geschäftsbetrieb stören würden. Dennoch sollte die qualitative Argumentation so weit wie möglich durch quantitative Analyse ausgeglichen werden. Was wäre die finanzielle Auswirkung einer größeren Datenschutzverletzung? Wären die Folgen immer gleich? Und wie hoch ist statistische Wahrscheinlichkeit, dass dies eintrifft?

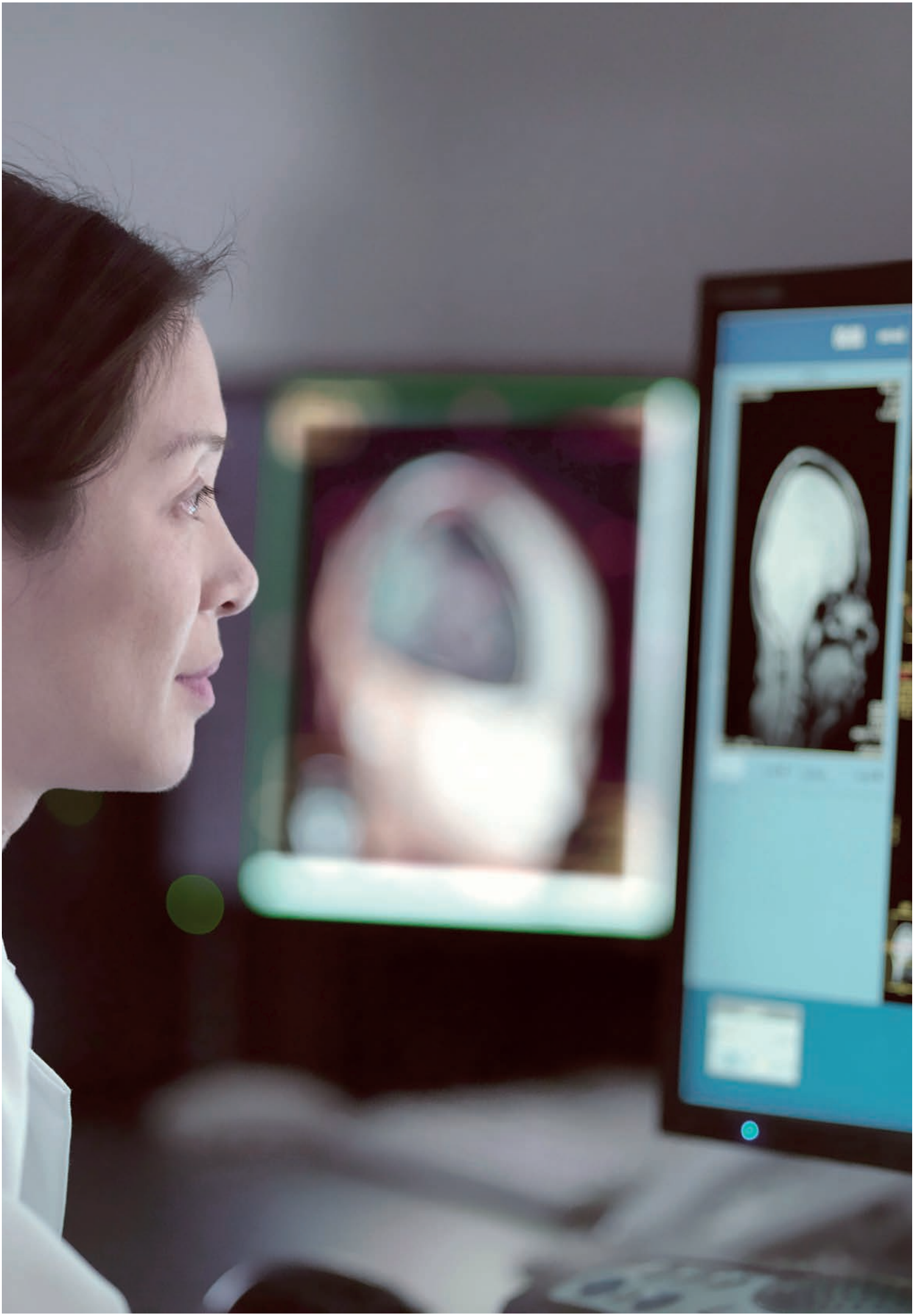
Menschen sind das schwächste Glied.
Der Umgang mit Daten ist zeitaufwändig und muss Teil des Tagesgeschäfts werden, um erfolgreich zu sein. Dies bedeutet, dass unternehmensweit Projektbetreuer und Verantwortliche für die Datenbestände (so genannte Dateneigentümer – Data Owner) ernannt werden müssen.

Viele Mitarbeiter versuchen jedoch, die ihnen – zusätzlich zu ihren täglichen Aufgaben – auferlegte Verantwortung für die Daten zu umgehen. Im schlimmsten Fall kommt es zur passiven Vermeidung, d.h. Mitarbeiter stufen das Risikopotential der Daten als geringer ein, um den „Ärger“ zu vermeiden, diese schützen zu müssen.

Um Cyberrisiken effektiv zu verwalten, müssen Unternehmen diese Reaktion von Mitarbeitern antizipieren und Maßnahmen ergreifen, um dies zu verhindern.

Eine schwere Datenschutzverletzung kann katastrophalen Schaden verursachen, denn sie

- untergräbt das Vertrauen der Kunden,
- zieht eine Überprüfung durch die Aufsichtsbehörden nach sich,
- beeinträchtigt den Betrieb
- und verursacht langfristige finanzielle Schäden.



Schützen Sie die falschen Daten?

Heutzutage sind Unternehmen nur so „gut“ wie ihre Daten. Je besser Ihre Informationen sind – seien dies Kunden- oder Arbeitnehmerdaten, Prozessaufzeichnungen oder tägliche Ausgabenrechnungen – umso besser können Sie vorausplanen, Entscheidungen treffen und Ihren Geschäftsbereich verwalten.

Alles, was wichtig ist, stellt eine Risikoquelle dar. Eine Kompromittierung sensibler Daten kann Reputationsschäden, finanziellen Verlust, hohe Geldstrafen (siehe Bereich „EU-Datenschutz-Grundverordnung“), Betriebsstörungen und Kundenabwanderung nach sich ziehen. Aus diesem Grund hat das Thema Informationssicherheit auf den Agenden der Unternehmen einen fixen Platz und wird regelmäßig unter den Top-Risiken der globalen Versicherungsgesellschaften[2] und des Global Risks Reports des Weltwirtschaftsforums aufgeführt.[3]

Unsere weltweite Umfrage bei 2.900 Unternehmen deutet jedoch darauf hin, dass viele kein klares Bild von ihren Daten oder deren grundlegenden Bedeutung haben. Weniger als zwei Drittel (65 %) der Unternehmen ergreifen Maßnahmen, um zu verstehen, welche Daten sie haben; nur etwa die Hälfte (56 %) weisen ihren Informationen ein Risikoprofil zu.

Verteidigung an falscher Stelle

Unsere Ergebnisse werfen eine einfache Frage auf: Verschwenden Unternehmen Zeit und Geld, um Informationen von geringem Wert zu schützen, während ihre wichtigsten Vermögenswerte einem hohen Risiko ausgesetzt sind, da sie keinen Überblick über ihren Datenbestand und deren Stellenwert haben?

Die Antwort lautet mit großer Wahrscheinlichkeit „Ja“. Etwa vier von fünf Befragten in unserer Umfrage (78 %) geben zu, dass sie dazu neigen, ihre Schutzmaßnahmen gleichmäßig auf alle Daten anzuwenden. Nur ein kleiner Teil gibt an besondere Schutzmaßnahmen vorzunehmen, um die wichtigsten Informationen zu schützen.

Ein Technologie-Vorstand einer international tätigen Bank, der für diesen Bericht befragt wurde, warnt vor den Gefahren, wenn keine spezifischen Kontrollen für Daten mit höherem Risiko eingerichtet werden. „Kritische Daten werden unter anderem auf das online Content-Management-System SharePoint geladen“, sagt er. „In vielen Unternehmen werden standardmäßige Zugänge zu kritischen Daten auf Plattformen eingerichtet.“

Das 80/20-Verhältnis bei Daten

Wir nehmen an, dass das Pareto-Prinzip beim Informationsrisiko anwendbar ist, wobei 20 % der Geschäftsdaten 80 % des Risikos darstellen. Tom Faulkner, Leiter der IT-Produktion bei CMC Markets, schätzt das Verhältnis als noch extremer ein. „Es gibt eine sehr dünne Oberschicht an Daten, vielleicht 5 % der Gesamtdaten, die auf höchsten Standards geschützt werden muss, da sie nicht verloren gehen darf“, sagt er. „Und dann haben wir eine bedeutsame Menge an Daten, die angemessen geschützt sein müssen.“

Es gibt ein bekanntes Sprichwort: „Alles zu schützen bedeutet nichts zu schützen.“ Es ist fast unmöglich, alle Systeme vollständig gegen Hackerangriffe zu sichern, also warum sich nicht auf die geringe Menge an Daten konzentrieren, für die Sicherheit absolut notwendig ist?

2. http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf / https://www2.chubb.com/TR-TR/_Assets/documents/20150707_EMERGING_RISK_ / https://www.grantthornton.global/globalassets/1.-member-firms/global/insights/Cyber Security-hub/value-of-data-hub/locking-down-the-value-of-data_report_grant-thornton.pdf
3. http://www3.weforum.org/docs/GRR17_Report_web.pdf

„Wenn Sie X Euro bezahlen müssen, um hochmoderne Firewalls, IPS und IDS-Geräte zu kaufen, die gesamtwirtschaftlichen Auswirkungen einer Datenschutzverletzung sich jedoch auf weniger als X Euro belaufen, dann ziehen es einige Unternehmen vielleicht vor, das Risiko auf sich zu nehmen und nicht in so teure Sicherheitsvorkehrungen zu investieren, oder stattdessen vielleicht weniger anspruchsvolle Cyber Security Frameworks zu installieren“, so John Kan, Chief Information Officer bei A*STAR in Singapur.

In diesem Sinne ist es unsere Überzeugung, dass Unternehmen ein strukturiertes Programm zur Bewertung und zum Verständnis ihrer Daten unter Verwendung eines Kategorisierungs- und Klassifizierungsprozesses durchführen sollten. Dann können sie ihre „Kronjuwelen“ identifizieren und einen wirksamen Schutz um sie herum aufbauen.

„Der erste Schritt besteht darin, zu verstehen, dass Ihre Informationswerte nicht gleichwertig sind. In einem zweiten Schritt werden die „Kronjuwelen“ identifiziert, die besonders geschützt werden müssen. Bei den restlichen Daten sind Grundschutzmaßnahmen völlig ausreichend.“

Georg Beham, Grant Thornton Österreich

EU-Datenschutz-Grundverordnung: Globale Auswirkungen

Ab 2018 werden die Kosten einer Datenschutzverletzung direkter und ziehen erhebliche finanzielle Konsequenzen nach sich. Im Mai 2018 werden auf Grundlage der EU-Datenschutz-Grundverordnung (DSGVO) Strafen in Höhe von bis zu 4 % des weltweiten Umsatzes gegen Unternehmen für den Verlust von Kundendaten verhängt. Sobald die DSGVO in Kraft tritt, ist es wahrscheinlich, dass andere Gerichtsbarkeiten weltweit ähnliche Regelungen einführen.

Der jüngste Cyberangriff gegen die Tesco Bank in Großbritannien betraf 9.000 Kundenkonten und führte dazu, dass die Bank insgesamt £ 2,5 Millionen zurückerstatten musste. Wäre die Sicherheitsverletzung nach dem Inkrafttreten der DSGVO eingetreten, so hätte die Bank möglicherweise mit einer Strafe von £2 Milliarden rechnen müssen – nur um das Ausmaß dieser Änderung deutlich zu machen.

Kronjuwelen: Gegenstand und Hintergründe

In der digitalen Welt ist es extrem schwierig, den Überblick über alle Daten zu behalten, die Ihr Unternehmen jeden Tag erzeugt und sammelt.

IBM geht davon aus, dass neun Zehntel der weltweiten Daten allein in den vergangenen zwei Jahren erzeugt worden sind.[4] Andere glauben, dass wir auf einem Planeten leben werden, der bis zum Jahr 2020[5] 40 Zettabyte Daten enthalten wird – schätzungsweise genug Lesestoff, um 50 Milliarden Menschenleben zu füllen.

Wie können Sie also Ihre Kronjuwelen und Ihre sensibelsten Daten in dieser Masse an Bytes identifizieren? Wie unterscheiden Sie Daten mit hohem, niedrigem und mittlerem Risiko? Und gegen welche Bedrohungen – von staatlich geförderten Agenten über organisierte Verbrecher, verärgerte Angestellten und „Hacktivisten“ bis hin zu unzufriedenen Jugendlichen – sollten Sie sich vorrangig schützen?

Vertraulichkeit, Integrität, Verfügbarkeit

Zunächst einmal ist es unrealistisch zu versuchen, jede Kalkulationstabelle, jedes archivierte E-Mail oder jede Datei Ihres Unternehmens einzuordnen. Der Prozess kann zudem nicht vollständig automatisiert werden: Es gibt Werkzeuge, die das Datenmanagement unterstützen, dennoch ist menschliches Urteilsvermögen immer erforderlich. Letztlich müssen Sie sicherstellen, dass Ihre Führungskräfte und Risikomanager aktiv die verschiedenen Arten von Daten betrachten, die sie besitzen – auf diese Weise können Sie die Daten isolieren, die einer genaueren Betrachtung bedürfen.

„Wir haben Fragebögen erstellt, damit unser Personal selbst eine Entscheidung treffen kann“, sagt der Technologie-Vorstand einer international tätigen Bank. „Es ist ein subjektiver Prozess. Am Ende des Tages ist es eine Person, die eine Entscheidung trifft.“

Im nächsten Abschnitt empfehlen wir Ihnen praktische Möglichkeiten, um sicherzustellen, dass sich Ihre Mitarbeiter an diesem Prozess beteiligen.

Viele Unternehmen übernehmen ein dynamisches Modell, welches Daten nach Vertraulichkeit, Integrität und Verfügbarkeit (confidentiality, integrity, availability – CIA) auswertet und dahingehend angepasst werden kann, dass Veränderungen der Wichtigkeit oder Bedeutung der Daten im Laufe der Zeit berücksichtigt werden.

„Strategiepapiere des Vorstands sind vertraulich, bis sie öffentlich gemacht werden, und müssen geschützt werden“, so Ewald Kager von Grant Thornton Österreich in Erklärung des CIA-Ansatzes. „Bezüglich Integrität können Informationen für jedermann zur Verfügung stehen – sie müssen jedoch präzise sein – der Aktienkurs der Wiener Börse ist ein gutes Beispiel. Verfügbarkeit bedeutet, dass diejenigen, die die Daten benötigen, diese jederzeit bekommen und verwenden können, wie zum Beispiel Marketinglisten.“

4. https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html
5. https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

Wie ein Angreifer denkt.
Eine weitere Möglichkeit zur Identifizierung Ihrer Risiken im Zusammenhang mit Ihren Daten ist, selbst wie ein Hacker zu denken und dann den maximalen Schaden zu untersuchen, den diese Risiken verursachen könnten.

„Das aktuelle Umfeld der Informationssicherheit entwickelt sich ständig weiter, mit neuen Bedrohungen und Schwachstellen", so Peter Kleebauer von Grant Thornton Österreich. „Führungskräfte müssen bereit sein, sich in Cyberkriminelle hineinzuversetzen, die Bedrohungen verstehen, die von diesen Gruppen ausgehen, und proaktive Strategien zum Schutz ihrer Geschäftsinteressen entwickeln."

Gibt es E-Mail-Verkehr, den ein früherer Angestellter veröffentlichen könnte, um seinen ehemaligen Vorgesetzten bloßzustellen? Gibt es geistiges Eigentum und Geschäftsgeheimnisse, die für eine ausländische Macht von Interesse wären? Und wie könnte ein Cyberkrimineller Ihre Daten verwenden, um Geld von Ihrem Unternehmen zu erpressen? Dies ist nur eine Auswahl der Fragen, die Sie sich stellen müssen.

Unternehmen in der Supply Chain- und Logistikbranche könnten mit einer Bedrohung ihrer Existenz konfrontiert werden, wenn Hacker ihre Daten blockieren oder manipulieren würden.

Dr. Ayman Omar, außerordentlicher Professor an der Kogod School of Business, hat viel Erfahrung im Bereich „Supply Chain" und versteht die Risiken. „Wenn Sie hochwertige Artikel versenden, können Personen auf die Versanddaten zugreifen und die physische Sendung angreifen", sagt Omar. „Wir haben Fälle erlebt, in denen die Lieferanten der Firma angegriffen wurden, mit dem Ziel, sie außer Gefecht. Dann wurde das Unternehmen erpresst Lösegeld zu bezahlen, um Verzögerungen zu vermeiden."

Ein Krankenhaus in den USA bietet ein weiteres Beispiel dafür, wie Hacker die Daten der Kerngeschäftsaktivitäten eines Unternehmens kompromittieren können. Cyberkriminellen gelang es Krankenakten der Patienten zu manipulieren und die Blutgruppen zu ändern. Die Täter wollten eine Lösegeld erpressen und erst nach der Zahlung als alle Krankenakten wieder in den ursprünglichen Zustand zu bringen. Hätte das Krankenhaus nicht eingewilligt, würden Patienten innerhalb einer halben Stunde die falschen Medikamente verabreicht bekommen. Diese Konsequenz wäre viel schlimmer als wenn das Krankenhaus zum Beispiel lediglich die Kreditkartendaten dieser Patienten verloren hätte.

Auch scheinbar unbedeutende Dateien können verwendet werden, um erhebliche Schäden zu verursachen, wie Ross Anderson, Professor für Sicherheitstechnik im Computerlabor der Universität Cambridge, erklärt: „Ein Unternehmen, das ich beraten habe, war der Ansicht, dass es nur eine Geldstrafe zahlen muss, wenn die Daten kompromittiert würden. Ich sagte: „Wie würden Sie sich fühlen, wenn alle Ihre E-Mails, mit all den Interna auf WikiLeaks oder Pastebin erscheinen würden?" Die Geschäftsführer wurden blass und Cyber Security wurde direkt an die Spitze ihres Risikoregisters gesetzt."

„Führungskräfte müssen bereit sein, sich in Cyberkriminelle hineinzuversetzen, die von solchen Gruppen ausgehenden Bedrohungen zu verstehen, und proaktive Strategien zum Schutz ihrer Geschäftsinteressen entwickeln."

Peter Kleebauer, Grant Thornton Österreich

Bedrohungen kritischer Daten nach Branchen

Ausgehend vom Erkenntnisstand der Branchenexperten von Grant Thornton werden nachstehend einige Bedrohungen nach Branchen aufgeführt.

Gesundheitswesen

- Blockierte Patientendatensätze, die zur Erpressung/ Lösegeldforderung benutzt werden
- Beschädigte Betriebsmittelinformationen, wie Steuerung der Klimaanlage in Krankenhäusern, die für Lösegeldforderungen verwendet werden
- Gestohlene oder blockierte Daten zur Arzneimittel-abgabe und -lagerung

„Alle Gesundheitsorganisationen sollten den Status Quo hinterfragen, bei dem IT-Funktionen einen Wertbeitrag darstellen und Wirtschaftsgut sind. Es beginnt mit dem Verständnis und der Priorisierung der Daten aus klinischer und geschäftlicher Sicht.

Im Gesundheitswesen können Menschen sterben, wenn ein kritisches System gehackt wird oder versagt. Die IT-Abteilung sollte sich stark auf die Aufklärung der End-User über die kontinuierliche Notwendigkeit von Datensicherheit konzentrieren."

Georg Beham, Grant Thornton Österreich

Finanzdienste

- Gestohlene oder blockierte Kundendatensätze, die für Betrug/Lösegeldforderungen benutzt werden
- Beschlagnahmte Markt-/ Handelsdaten, die zu Betriebsstillstand führen
- Einführung von Algorithmen, um automatisierte Handelsaktivitäten zu deaktivieren/zu verzerren

„Bei globalen Finanzdiensten steigt die Abhängigkeit von digitaler Technologie, während sich Kriminelle mehr und mehr auf Systemangriffe konzentrieren, wie die SWIFT-Vorfälle und Bedenken im Zusammenhang mit Zahlungssystemen zeigen. Diese Themen, gepaart mit dem klaren regulatorischen Fokus auf Cyberrisikomanagement, bedeuten, dass viele damit kämpfen, effektiv zu reagieren.

Finanzdienstleistungsorganisationen sollten sich zunächst auf den Aufbau eines robusten, risikobasierten Cybersicherheit-Programms konzentrieren. Dies wird dazu beitragen, strategische Ziele zu erreichen und gleichzeitig den regulatorischen Anforderungen gerecht zu werden. Letztendlich können Sie Innovationen beschleunigen, indem Sie sich zuerst auf Cybersicherheit konzentrieren."

Mike Harris, Grant Thornton Irland

Energiedienstleister

- Korruption von GIS-Daten, die den Standort von Gas oder Strom im Netzwerk verfolgen
- Sicherheits- und Kartendaten von Ölquellen blockiert/für Lösegeldforderungen verwendet

„Die Idee einer voll vernetzten Welt, in der alle Systeme und Menschen miteinander verbunden sind und jedes System online zugänglich ist, ist extrem gefährlich. Denken Sie an Dämme oder Kernkraftwerke – Angreifer haben bewiesen, dass sie sogar höchste Sicherheitseinrichtungen überwinden können. Unter anderem sind diese kritischen Infrastruktur-Einrichtungen leichte Beute für Angreifer, deren einziges Ziel es ist, Chaos anzurichten."

Philipp Mattes-Draxler, Grant Thornton Österreich

Öffentlicher Sektor

- Diebstahl von Daten, die für die Bereitstellung von Notfalldiensten notwendig sind
- Korruption/Manipulation von Wirtschafts- und Handelsdaten durch Agenten im Ausland
- Diebstahl von Staatsgeheimnissen

Konsumgüter

- Diebstahl von Fertigungsprozessinformationen
- Korruption oder Diebstahl von Transport- und Lieferkettendokumentation
- Gestohlenes geistiges Eigentum und F&E-Daten

„Die Menge sensibler Daten, die von Regierungsstellen / Öffentlichem Sektor gespeichert, verwaltet und verarbeitet wird, ist um ein Vielfaches größer als jenes großer Unternehmen weltweit.

Auch bei einzelnen Regierungsbehörden kann es vorkommen, dass Informationen gesichert werden müssen, wie zum Beispiel personenbezogene Informationen, Gesundheitsdatensätze, Patente und Geschäftsgeheimnisse sowie Bankinformationen. Angesichts all dessen und mit begrenzten Ressourcen, um in Programme und Cyberexpertise zu investieren, müssen Behörden von einem Compliance-Ansatz mit Checkliste zu einem risikoorientierten, kontinuierlichen Monitoring-Modell wechseln."

Peter Kleebauer,
Grant Thornton Österreich

Immobilien und Bauwesen

- Korruption/Diebstahl von Baustoffspezifikationen zur Erpressung von Lösegeld
- Korruption/Diebstahl von Transport- und Lieferkettendokumentation
- Einführung „inhärenter Mängel" in Baupläne, um zukünftige Schwachstellen in der Struktur zu schaffen

Reisen, Freizeit und Tourismus

- Diebstahl/Korruption von Reisepass- und Visa-Daten für betrügerische Zwecke
- Gestohlene oder blockierte Daten, die für öffentliche Transportmittelsysteme benötigt werden
- Beschädigte/blockierte Verkehrsüberwachungs- oder Steuerdaten
- Technologie, Medien und Telekommunikation
- Kompromittierte Kundendatensätze
- Störung der wichtigsten Kommunikationsnetze
- Diebstahl von geistigem Eigentum

„Mit Technologie im Epizentrum des Unternehmens- und Konsumentenlebens sind Technologieunternehmen ideale Ziele für Cyberangriffe. Sie haben die doppelte Herausforderung, Ihre Vermögenswerte zu schützen, während Sie Ihre Produkte und Infrastrukturen stärken, die das Rückgrat für E-Commerce und soziale Netzwerke bilden.

Der riesige Wert, der von Daten generiert und transportiert wird, muss bei jedem Schritt geschützt werden."

Ewald Kager, Grant Thornton Österreich

Qualitative und quantitative Bewertung ausgleichen

Eine konsistente, qualitative Bewertung der Daten ist wichtig, aber die quantitative Bewertung sollte dabei nicht vernachlässigt werden. Diese umfasst eine Einschätzung der finanziellen Auswirkungen einer Datenschutzverletzung sowie die Berechnung der Wahrscheinlichkeit ihres Eintreffens.

Omar von der Kogod School of Business glaubt, dass viele Unternehmen zu viel Wert auf die subjektive Analyse legen. „Top-Geschäftsführer werden gebeten, die Risiken des Unternehmens auf einer Skala von null bis fünf einzustufen“, so Omar. „In Wirklichkeit ist das kein bisschen genauer, als einfach gar nichts zu tun. Sie quantifizieren damit nicht die Wahrscheinlichkeit, dass dieses Risiko eintritt oder die finanziellen Auswirkungen. Wenn Sie sagen, das Schadensausmaß ist „drei“, was bedeutet drei?“

Er fügt hinzu, dass die Durchführung einer quantitativen Bewertung der Auswirkungen und der Wahrscheinlichkeit eine Analyse der Häufigkeit des Auftretens innerhalb des Unternehmens sowie bei anderen in der Branche einschließt.

Checkliste:

Die potenziellen „Daten-Kronjuwelen“

- ☐ Forschungs- und Entwicklungsdaten
- ☐ Regulierte Daten: Gesundheitsdaten, Finanztransaktionsdaten
- ☐ Kreditkartendaten und andere Zahlungsinformation
- ☐ Firmeneigene Verfahren
- ☐ E-Mail-Daten mit Kommunikationsdaten der Geschäftsleitung
- ☐ Geschäftsgeheimnisse
- ☐ Personenbezogene Information
- ☐ Geistiges Eigentum
- ☐ Finanz und nicht finanzielle Information

Erfolgsbarrieren

Viele Unternehmen verstehen die Bedeutung ihrer Daten nicht oder verwalten die damit verbundenen Risiken nicht erfolgreich. Weniger als zwei Drittel (65 %) versuchen die Daten, die sie besitzen, vollständig zu verstehen und nur die Hälfte (56 %) weist diesem kritischen Betriebsvermögen ein Risikoprofil zu.

Die Verwaltung von Daten ist nicht einfach und sollte nicht auf die leichte Schulter genommen werden. Beim Versuch ihre Daten zu verstehen, müssen Unternehmen mehrere Herausforderungen meistern.

1. Bestandsrisiken und neue Bedrohungen

In vielen Unternehmen wurde die Risikomanagement-Abteilung eingeführt, um eine definierte Liste der versicherbaren Geschäftsrisiken zu verfolgen, zu messen und zu entschärfen. Oft sind diese Teams bei der Verwaltung von sich schnell weiterentwickelnden, virtuellen Risiken weniger erfahren.

Infolgedessen können Datenverletzungen und Infiltrationen durch Hacker nicht wie andere Bedrohungen in die Risiko-minderungsstrategie eingebunden werden. Dies könnte ein Erklärungsansatz dafür sein, warum eine relativ bescheidene Anzahl von Unternehmen weltweit ihren Daten ein Risikoprofil zuweist.

„Cyber ist ziemlich neu und war noch nie Teil der etablierten Risikoorganisation“, so der Technologie-Vorstand einer international tätigen Bank. „Die frühere Risikoorganisation hat keine Cyberszenarien, Cyberbedrohungsmodelle oder Cyberangriff-Szenarien berücksichtigt. Wir haben erst vor kurzem begonnen, in eine starke Cybergruppe zu investieren.“

2. Passive Vermeidung: Datenbesitzer vermeiden zusätzliche Arbeit

Wie bei jeder prozessgesteuerten internen Initiative ist es wahrscheinlich, dass sich Mitarbeiter, die bereits mit ihren alltäglichen Aufgaben ausgelastet sind, der Vergabe neuer Aufgaben durch das Unternehmen zunächst widersetzen und ihre neuen Aufgaben nicht erfüllen.

Einer der leitenden Angestellten, die wir für diesen Bericht befragten, stimmt zu, dass viele Mitarbeiter letztlich ihrer eigenen Arbeit den Vorrang geben. „Das führt dazu, dass die Daten überall verstreut sind“, sagt er. „Das hängt damit zusammen, dass Angestellte im Rahmen der Ausführung ihrer Aufgaben Datenexporte der Einfachheit halber lokal gespeichert und per E-Mail weitergeschickt haben.“

Umso beunruhigender war die Feststellung einer befragten Führungskraft, dass Mitarbeiter bei der Klassifizierung ihrer Daten bewusst irreführend vorgehen. „Wir haben die Datenkategorisierung den Eigentümern der Dienstleistungsprozesse überlassen, mussten jedoch feststellen, dass 70 % das Risiko absichtlich als geringer einstuften, um die Umsetzung von Kontrollen zu umgehen. Wir haben deshalb eine Arbeitsgruppe eingerichtet, um die Antworten vor deren Einspeisung ins System zu verifizieren.“

Es ist schwierig, die richtige Balance zu finden. Wenn Sie bei der Kategorisierung zu rigoros vorgehen und sehr starre Kontrollen einführen, riskieren Sie die Entwicklung einer unangenehmen Arbeitskultur, die zum Arbeitskräfteabgang führt. Wenn Sie jedoch in der Implementierung zu sanft sind, erleben Sie „passive Vermeidung“, bei der Angestellte Richtlinien ignorieren oder etwas als niedrige Priorität markieren, um sich das Leben leichter zu machen.

3. Die wesentlichen (oder die meisten leitenden) Mitarbeiter sind außen vor

Wenn Sie nicht genug Unterstützung durch das Top-Management haben, wird eine unternehmensweite Da-tenschutzinitiative wahrscheinlich fehlschlagen. Das liegt nicht nur daran, dass die eine Vorbildfunktion ausüben soll,

um dem Programm ein angemessenes Maß an Bedeutung zu verleihen, sondern vor allem daran, dass sich die an der Bewertung der Daten beteiligten Personen über ihre breitere strategische Relevanz im Klaren sind. Über die Führungsebene hinaus kann das auch bedeuten, Angestellte aus allen Abteilungen des Unternehmens einzubinden. „Sie brauchen Bereiche wie Operations, Marketing, Finanzen und IT“, sagt Omar. „IT-Leute fragen: „Mit welchen Auswirkungen werden wir zu tun haben, wenn ein Angriff stattfindet?“ Operations wird ihnen von Produktionsverzögerungen erzählen, was wiederum höhere Sicherheitsbestände im Inventar bedeuten kann. Und dann sagt jemand der Finanzabteilung, dass Sicherheitsbestände jeglichen Profit im Keim ersticken.“

Ein Teil des Problems ist, dass die Gewohnheit der letzten Jahrzehnte, Wissen über funktionale Einheiten hinweg zu teilen, die umfassende Einschätzung der Auswirkungen einer Sicherheitsverletzung erschwert hat. „Das Verständnis muss aus verschiedenen Abteilungen und verschiedenen Funktionsbereichen kommen“, so Omar.

4. Unbeständigkeit in der Anwendung

Trotz Orientierungshilfen wie dem CIA-Modell (siehe Abschnitt 3) und den Informationssicherheitsvorgaben nach ISO 27001 ist es für große Unternehmen schwierig, Beständigkeit darin zu erreichen, wie ihre Mitarbeiter mit Daten umgehen. Dieses Problem wird durch die Tatsache verschärft, dass sich das Risiko eines Datensatzes im Laufe der Zeit ändern kann, abhängig von dessen Relevanz für aktuelle Geschäftsprioritäten. „Wir haben Kontrollverfahren, die bei der Bestimmung helfen, ob etwas vertraulich ist oder nicht“, sagt einer der leitenden Angestellten, mit denen wir für diese Studie gesprochen haben. „Aber Sie werden niemals eine Liste erstellen können, die alle Daten beinhaltet. Manchmal ist es schwierig zu verstehen, was auf dieser Liste stehen sollte.“

5. Unterschätzung der Bedrohung

Manche Unternehmen sehen den Verlust von Kundendaten und die Reputationsschäden, die durch negative Medienberichterstattung verursacht werden, als die Hauptbedrohungen im Rahmen des Cyberrisiko-Managements an. Die Schäden für die Unternehmen waren jedoch in einigen Fällen geringer als erwartet, was dazu führte, dass manche Unternehmen dazu neigen, mögliche Schäden durch Hackerangriffe zu verharmlosen.

Sony ist ein gutes Beispiel, so Chris Hankin, Direktor des Instituts für Sicherheitswissenschaften und Technik am Imperial College London. „Die Sicherheitsverletzungen bei Sony hatten einen kurzfristigen Effekt auf den Aktienkurs und den Kundenstamm“, erklärt er. „Aber die Kunden haben sich sehr schnell damit abgefunden, dass ihre Daten verloren gegangen sind. Sie blieben weiterhin bei Sony, weil sie das Unternehmen und die Dienste immer noch geschätzt haben.“

Hankin erkennt jedoch an, dass Reputationsschäden für ein Unternehmen wie seines das Ende bedeuten könnte. „Es würde das Ende einer Universität bedeuten, wenn die Studenten nicht mehr kämen. Die Studentendatenbanken sind Teil unserer Kronjuwelen. Wenn wir den Ruf hätten, diese Daten nicht angemessen zu schützen, wenn wir große Mengen an Datensätzen verlieren würden, würden die Studenten uns nicht mehr vertrauen und sich nicht mehr bewerben, und wir könnten als Universität nicht mehr funktionieren.“

Wann eine Sicherheitsverletzung hilfreich sein kann

Mehrere der Befragten sind der Auffassung, dass eine Sicherheitsverletzung auch eine positive Erfahrung sein kann, weil sie das Management auf das Ausmaß des Problems aufmerksam macht und Schwächen aufzeigt. „Bei Unternehmen, die Opfer von Cyberattacken wurden, bemerkten wir, dass sie später Budget erhielten, um sicherere Systeme zu entwickeln und zusätzliche Cyber Security-Sensibilisierungsprogramme einzuführen“, so Kan von A*STAR.

David Pollino, Senior Vice President und stellvertretender Chief Security Officer bei der Bank of the West USA glaubt, dass aus einem relativ kleinen Vorfall positive Ergebnisse entstehen können. „Sie können gut vorbereitet sein, aber bis Sie nicht mindestens einmal Opfer eines Cyberangriffs wurden, werden Sie nie wirklich wissen, ob alles perfekt umgesetzt wird“, sagt er. „Es gibt immer Verbesserungsspielraum.“

Unsere Erfahrung bestätigt die Auffassung, dass eine kleine Sicherheitsverletzung manchmal notwendig ist, um den Vorstand zu größerem Interesse zu bewegen, was wiederum einen strukturierten Ansatz zur Datensicherheit garantiert.ke Harris von Grant Thornton Irland. „Wenn der Vorstand beteiligt ist, bedeutet das Disziplin und strukturiertes Projektmanagement.“

Der Weg nach vorne: Drei Schritte zu einem besseren Datenverständnis

Unternehmen müssen lernen, ihre Daten besser zu verstehen, sehen sich aber auf dem Weg dahin mit vielen Hürden und Herausforderungen konfrontiert. An dieser Stelle skizzieren wir unsere Empfehlungen, um Unternehmen dabei zu helfen, die Bedeutung ihrer Daten zu erkennen und letztlich einen ausgereifteren Ansatz für das Informationsrisikomanagement zu erreichen.

1 SCHRITT 1: Verantwortlichkeiten und Zuständigkeiten klären.

Informationssicherheit sollte wie ein Teil des unternehmensweiten, konsequent angewendeten Risikomanagements behandelt werden. Das impliziert die Ernennung eines systemweiten Eigentümers (oft der Chief Revenue Officer oder Chief Financial Officer, wenn es keinen speziellen Chief Information Security Officer gibt), sowie eines Eigentümers „vor Ort" auf operativer Ebene (z.B. lokaler Informationssicherheitsbeauftragter). **Das geht mit der bewussten Auffassung einher, dass Ihre Daten ein strategischer Vermögenswert sind, für welche das Risiko bestimmt werden sollte und welche in das Risikoregister aufgenommen werden sollten.**

„Der CFO, vor allen anderen Führungskräften, führt Cybersicherheitsbemühungen an", sagt Georg Beham von Grant Thornton Österreich. „CFOs beschaffen in der Regel Versicherungsprodukte und haben üblicherweise die meiste Interaktion mit anderen Führungskräften in Bezug auf Unternehmensrisiken." Andrew Harbison von Grant Thornton Irland glaubt, dass einer der Vorteile der Zuweisung von alltäglicher Verantwortung darin besteht, dass sich Dateneigentümer bewusst sind, dass sie zur Rechenschaft gezogen werden, wenn eine Verletzung stattfindet. „Menschen reagieren besser auf persönliche Risikovermeidung als auf direkte Bedrohungen", sagt Harbison.

2 SCHRITT 2: Informationsrisikomanagement ins Konzept integrieren („security by design“)

„Sie müssen Sicherheit schon in die Konzeption integrieren“, sagt Nick Oldham, Anwalt für Datensicherheit und Privatsphäre bei der internationalen Anwaltskanzlei King & Spalding. „Sicherheit und Privatsphäre sind Komponenten, die Unternehmen oft erst am Ende eines neuen Projekts berücksichtigen, was dann später zu Problemen führt.“

Der VP im Bereich Technologie bei einer globalen Bank ist auch der Meinung, dass es besser ist, Datensicherheit in einem frühen Stadium einzubetten. „Wir möchten, dass dies in viel größerem Ausmaß im Entwicklungszyklus enthalten ist“, sagt er. „Wir erstellen Bedrohungsszenarien und führen Designüberprüfungen durch, wo Sie iterativ auf die Bewertung aufbauen; gefolgt von einem Evaluationstest durch IT- Sicherheitsexperten.“

Funktionsübergreifende Einsicht

„Security by Design“ besteht aus mehreren Teilen. Man stellt sicher, dass eine Reihe von Funktionen in den laufenden Bewertungsverfahren und im Umsetzungsprozess involviert sind und nicht nur die einzelnen Dateneigentümer. „Das gesamte Unternehmen muss bei Unternehmensrisikobewertungen und Auswirkungsanalysen von Cyberattacken beteiligt sein – und nicht nur die IT-Abteilung allein“, so Kan von A*STAR. „Es muss eine Kombination aus Abteilungen, Bereichen und Geschäftseinheiten sein, die in einem multidisziplinären Team zusammenkommen, um die Szenarioplanung und die Folgenabschätzung solcher Vorfälle vorzunehmen.“

Datenlöschung als Standard

Verantwortungsvolle Datenlöschung verringert die Wahrscheinlichkeit einer Datenschutzverletzung. „Eine Datenklassifikationsrichtlinie legt einerseits fest wie Daten zu klassifizieren sind und andererseits wie klassifizierte Daten zu behandeln sind“, sagt Peter Kleebauer von Grant Thornton Österreich.

Sunil Chand von Grant Thornton Kanada glaubt, dass Datenvernichtung in alle vereinbarten Standards der Datennutzung integriert werden sollte. „Die Nützlichkeit Ihrer Daten wird durch die Geschäftsbedürfnisse, die Gesetzgebung, die Regulierung und die Frage, ob Sie sich in einem Rechtsstreit befinden, vorgegeben“, so Chand. „Der beste Ansatz, der überdies recht einfach ist, ist die Einführung einer Datenlöschpolitik mit begleitendem Handbuch oder automatisierte Kontrollen als Standard, es sei denn, die Informationen werden derzeit oder zukünftig noch benötigt.“

3 SCHRITT 3: Kommunikation und Schulung gestalten

„Der beste Weg, Ihren Mitarbeitern zu helfen, die Wichtigkeit von Cyber-Bedrohungen zu verstehen, ist ihnen auf menschlicher Ebene zu begegnen und technischen Jargon zu vermeiden“, so Kan. „Sie müssen IT-Teams aufbauen, die die Kommunikationslücke zwischen Geschäftsnutzern und technischen Werkzeugen durch die Nutzung von Laiensprache schließen können. Es ist wie das Einmaleins menschlicher Beziehungen.“

Für Anderson von der Universität von Cambridge ist erfolgreiche Kommunikation mit besserem Geschichtenerzählen verbunden. „Unternehmen sollten nicht über Daten sprechen“, sagt Anderson. „Sie sollten darüber reden, was in menschlicher Hinsicht schiefgehen kann. Das Gehirn ist dafür ausgelegt, Geschichten zu erzählen, und wenn Sie anfangen, über Datenkategorien zu sprechen, schalten die meisten ab.“ Oldham von King & Spalding stimmt zu und schlägt vor, dass Unternehmen ihre Botschaften anpassen, um über die persönlichen Anliegen und Prioritäten der Einzelnen zu sprechen. „Kommunikation muss von der Vorstandsebene bis hin zum technischen

Team frei fließen. Das muss so vermittelt werden, dass die Leiter der Rechtsabteilung die Botschaft in rechtliche Handlungen und geschäftsorientierte Führungskräfte in geschäftliche Angelegenheiten umsetzen können."

Laufende Weiterbildung

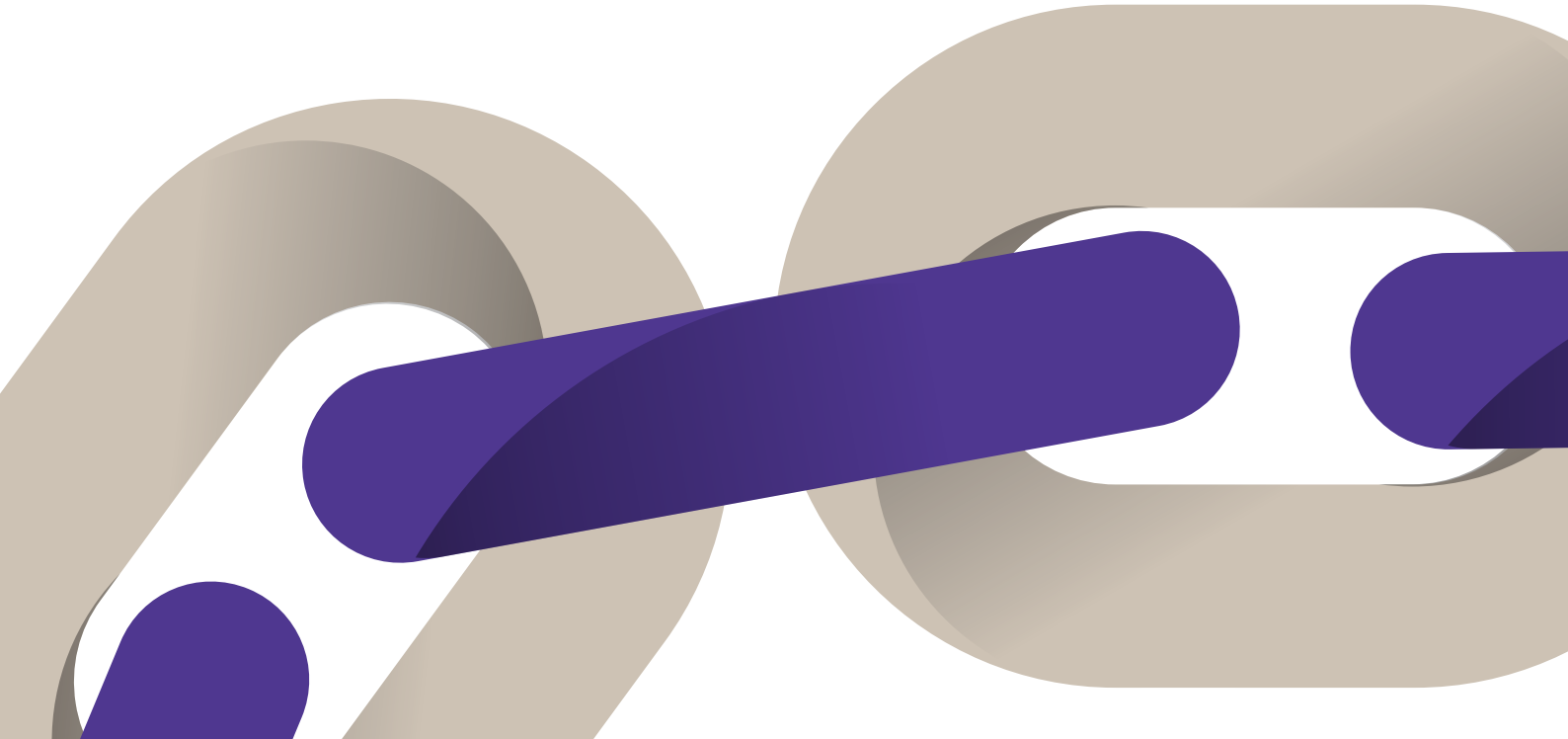
„Wenn ein Unternehmen darauf vertrauen muss, dass Mike in der Kreditorenbuchhaltung nicht auf einen Link klickt, dann ist dies schon der Anfang vom Ende des Unternehmens", so Chris Bronk, außerordentlicher Professor an der Universität Houston. „Phisher sind sehr raffiniert. Zu erwarten, dass Angestellte eines Unternehmens gewiefter als Kriminelle vorgehen, ist als würden Sie von anderen Menschen erwarten, listiger als Autodiebe zu sein."

Weiterbildung spielt eine wesentliche Rolle bei der Verbesserung des Bewusstseins und der Widerstandsfähigkeit der Mitarbeiter und hilft auch, das „Einmaleins menschlicher Beziehungen" von Kan umzusetzen – vor allem um sicherzustellen, dass der Gedanke an Datenrisiken in Fleisch und Blut übergeht.

„Jeder Hacker bzw. Angreifer wird Ihnen sagen, dass der schwächste Punkt in einem System der Mensch ist", warnt Peter Kleebauer von Grant Thornton. „Also ist das Schlagwort hier Schulung, Schulung und nochmals Schulung. Ein Unternehmen, mit dem ich gearbeitet habe, verwendete die Farben grün, gelb und rot zur Klassifizierung von Daten. Aber dann wurde letztendlich alles rot markiert, also mussten sie purpur für Daten einführen, die noch gefährdeter als die „roten" eingestuft wurden. Wenn das passiert, muss man sich wirklich mit dem Team zusammensetzen und erklären, wie man Daten richtig einstuft."

Die Vorteile jenseits der Cyber Security

Die Vorteile eines besseren Datenverständnisses gehen weit über effektive Cyber Security hinaus. Beham sagt, dass Unternehmen ihre Mitarbeiter dazu anregen können, ihre Daten zu verstehen, indem sie auf den zusätzlichen Wert dieser hinweisen. „Wenn ich in den letzten 15 Jahren eine Sache gelernt habe", sagt er, „dann, dass es sich bei Cyber Security um ein Wirtschaftsthema handelt."



Zusammenfassend

Die meisten Unternehmen erkennen, dass Cyberrisiken mit der zukünftigen Nutzung neuer Technologien zunehmen werden und dass sie mit der Bedrohung besser umgehen müssen.

Cyberrisiken müssen mit kontinuierlicher Verbesserung angegangen werden. Vor allem sollten Daten als wichtiges Betriebsvermögen gesehen werden – doch unsere Untersuchung deutet darauf hin, dass viele Unternehmen ihre Daten nicht als solches wahrnehmen. Es wird nicht genug unternommen, um zu verstehen, was sie haben und wie sie es schützen können. Auch wenn sie Maßnahmen ergreifen, um den Schutz der Daten zu verbessern, tun sie dies oft mit älteren Tools und Ansätzen, die nicht ausreichen, um das Risiko eines Datenschutzvorfalls zu messen, zu verwalten und zu bepreisen.

Ein umsetzbarer und effektiver Ansatz ist jedoch sicherlich in Reichweite, wie wir in diesem Bericht dargelegt haben. Zunächst müssen Unternehmen akzeptieren, dass ihre Daten zu umfangreich und zu wichtig sind, um sie zu ignorieren.

Darüber hinaus müssen Sie pragmatisch sein. Wenn Sie davon ausgehen, dass jemand irgendwann einen Weg finden wird, in Ihre Systeme zu gelangen, werden Sie sicherstellen wollen, dass Ihre wertvollsten Daten unangreifbar bleiben.

Letztendlich bedeutet dies, zu verstehen, was je nach Branche, Risikoprofil und Geschäftszielen Ihre Kronjuwelen sind, und ihnen spezifische Kontrollen zuzuordnen. Dies ist vielleicht nicht einfach oder nur begrenzt möglich, aber sicher ein unverzichtbarer Teil von Risikomanagement im digitalen Zeitalter.

„Wissen entsteht aus rohen Daten und Algorithmen. Vergleiche von Daten mit Öl oder Gold sind irreführend, weil Daten mit marginalen Kosten kopierbar sind. Daher wird zukünftig – anders als bei physischen Ressourcen – nicht die Knappheit, sondern die Kontrolle über Datenkopien entscheidend sein.“

René Mayrhofer, Johannes Kepler Universität Linz

Kontakt

Wir helfen unseren Kunden, sich auf Cyber-bedrohungen vorzubereiten, kontinuierlichen Schutz sicherzustellen, effektiv auf Angriffe zu reagieren und Veränderungen einzuleiten, um ihr Leistungsvermögen im Bereich der Cyber Security zu verbessern.

Bitte wenden Sie sich an unser Team von Spezialisten, um zu erfahren, wie Informationsmanagement in Ihrem Unternehmen verbessert werden könnte, um Cyberrisiken zu minimieren.

Georg Beham, MSc
T +43 1 26 262 31
E georg.beham@at.gt.com

Mag. (FH) Ewald Kager
T +43 1 26 262 11
E ewald.kager@at.gt.com

Grant Thornton Unitreu Advisory GmbH
Rivergate Handelskai 92, Gate 2, 7A
1200 Wien

Geschäftsstelle:
Gewerbepark Urfahr 6,
4040 Linz

E info@at.gt.com
W grantthornton.at

Um mehr über Cyber Security zu erfahren und wie wir Sie unterstützen können besuchen Sie uns unter grantthornton.at/cyber-security

IBR Forschungsmethodik

Der Grant Thornton International Business Report (IBR) gibt Einblick in die Ansichten und Erwartungen von mehr als 10.000 Unternehmen in 36 Wirtschaftszweigen

pro Jahr. Fragebögen werden in die jeweiligen Landessprachen übersetzt, wobei jedes teilnehmende Land die Möglichkeit hat, neben dem Kernfragebogen auch eine kleine Anzahl von länderspezifischen Fragen zu stellen. Die Feldforschung erfolgt vierteljährlich, vorwiegend telefonisch. Der IBR bietet einen Überblick über börsennotierte sowie private Unternehmen.

Die Daten für diesen Bericht wurden in Interviews mit mehr als **2.900** Vorstandsvorsitzenden, Geschäftsführern, Vorständen oder sonstigen Führungskräften in der Zeit von Oktober bis Dezember 2016 gesammelt.

Danksagungen

Neben der oben genannten qualitativen Forschung haben wir mit Longitude zusammengearbeitet, um Anfang 2017 eingehende Interviews mit Cyber Security-Spezialisten im Grant Thornton-Netzwerk sowie externen Führungskräften und Vorstandsmitgliedern durchzuführen.

Wir danken den folgenden Personen für ihre Zeit und ihre Einsichten in diesem Bericht:

- Ross Anderson, Professor für Sicherheit, Computerlabor an der Universität von Cambridge
- Chris Bronk, Assistenzprofessor, Universität Houston
- Tom Faulkner, Leiter IT-Produktion, CMC Markets
- Chris Hankin, Direktor des Instituts für Sicherheitswissenschaft und Technik, Imperial College London
- John Kan, Chief Information Officer, A*STAR
- René Mayrhofer, Head of the „Institute of Networks and Security, Johannes Kepler Universität Linz
- Nick Oldham, Anwalt für Datensicherheit und Privatsphäre, King & Spalding
- Ayman Omar, außerordentlicher Professor und wissenschaftlicher Mitarbeiter im Kogod
- Cyber Security Governance Center, Kogod School of Business, American University
- David Pollino, Senior Vice President und stellvertretender Chief Security Officer, Bank of the West
- Dem IT-Direktor einer Investment-Management-Firma, auf Wunsch anonym
- Dem Vice President im Bereich Technologie bei einer globalen Bank, auf Wunsch anonym

grantthornton.at