Praxisrelevantes Wissen zum Thema Datenschutz

Forcepoint

Broschüre

Einführung in die Systemlandschaft

Die Aspekte Datensicherheit und Unternehmensleistung sind seit jeher untrennbar miteinander verbunden. Schließlich ist der Schutz von Geschäftsgeheimnissen vor unbefugtem Zugriff das A und O des Wettbewerbsvorteils – egal, ob es sich um interne Verfahren, relevantes geistiges Eigentum oder eine Rezeptur handelt.

Heute ist das Thema allerdings komplexer denn je. Ca. 90 % aller weltweit verfügbaren Daten sind innerhalb von nur zwei Jahren entstanden.[1] Zudem werden u. a. infolge der vermehrten Nutzung mobiler Geräte, der zunehmenden Verzweigung von Kunden- und Dienstleisterbeziehungen und des Einsatzes von ortsunabhängigen bzw. Roaming-Mitarbeitern Daten von immer mehr Personen an immer mehr Orten gespeichert und abgerufen – und das rund um die Uhr.

Daten am Arbeitsplatz sind relevanter denn je und öffentlichkeitswirksame Datenschutzverletzungen machten die Datensicherheit letztendlich zu einem eigenständigen Business Case. Ein wesentlicher Faktor sind hierbei die finanziellen Auswirkungen – eine Datenschutzverletzung kostet im Schnitt 3,26 Millionen US-Dollar.[2] Das heißt konkret: Jeder Verstoß gegen den Datenschutz kann einer Unternehmensmarke nachhaltig schaden und dem Vertrauen der Kunden entgegenwirken.

Stark regulierte Industriezweige wie das Gesundheits- und Finanzwesen unterliegen schon länger gesetzlichen Verpflichtungen zur Sicherung sensibler Daten. In letzter Zeit stiegen jedoch die öffentliche Wahrnehmung und das allgemeine Bewusstsein für Datensicherheit, woraufhin neue gesetzliche Regelungen zur Erfassung, Verarbeitung und Speicherung von Daten in Unternehmen erarbeitet wurden, wie zum Beispiel der malaysische Personal Data Protection Act (PDPA), die Datenschutz-Grundverordnung der EU, die australischen Datenschutzregelungen und der California Consumer Privacy Act (CCPA). Allein durch die Existenz dieser Regelungen muss sich jede Organisation intensiv mit dem Thema Datenschutz auseinandersetzen, egal, ob sie bestimmten Vorschriften unterliegt oder nicht.

3,26 Millionen US-Dollar

Durchschnittliche Kosten einer Datenschutzverletzung[2]

2.600–10.000

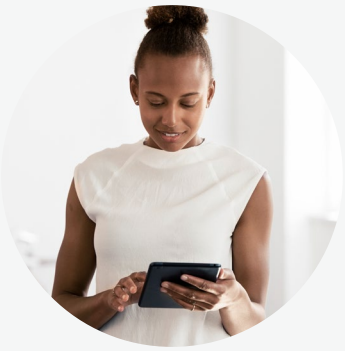
Durchschnittliche Anzahl sensibler Datensätze, die pro Datenschutzverletzung verloren gehen[2]

68 %

aller Datenschutzverletzungen bleiben monatelang unerkannt[2]

Denn eines lässt sich nicht leugnen: Unternehmen und ihre Mitarbeiter können in der heutigen Geschäftswelt nur bestehen und Leistung erbringen, wenn sie in puncto Datensicherheit umdenken. Der stetige Wandel ist zur Normalität geworden – und in dieser Normalität kann ein reaktives Vorgehen nicht länger den nötigen Schutz bieten. Finden wir heraus, wie wir uns dem Thema Datenschutz proaktiv stellen können – und warum dieser Ansatz für heutige Unternehmen der Goldstandard ist.

Ca. 90 % aller weltweit verfügbaren Daten sind innerhalb von nur zwei Jahren entstanden.[1]



Datensicherheit ist relevanter denn je

In vielen Abteilungen für Datensicherheit folgt die Arbeit immer demselben Muster: Eine Warnung geht ein, wird geprüft und der Schaden wird behoben – es nimmt kein Ende. Das Problem: Durch unflexible Richtlinien werden auch Aktivitäten mit geringem Risiko erfasst, was zu Fehlalarmen führt. Deren Auswertung kostet Zeit – Zeit, die durch den ohnehin sehr großen Arbeitsaufwand in diesen Abteilungen kaum vorhanden ist.

Datenschutztechnologien, die den Kontext von Cyber-Aktivitäten einbeziehen können, nehmen den verantwortlichen Mitarbeitern einen Teil der Arbeit ab. Durch das Herausfiltern harmloser Meldungen kann der Fokus auf die wirklich bedrohlichen Vorfälle gelegt werden. Durch ein verbessertes Zeitmanagement können die Sicherheitsteams zudem ihre eigene Rolle innerhalb des Unternehmens aufwerten und dieses proaktiv in eine sicherere und effizientere Zukunft führen. Das einfache Durchsetzen von Regeln gehört dann der Vergangenheit an.

Mehr Zeit für berufliche Weiterentwicklung

Wenn Datenschutzexperten sich nicht mit Fehlalarmen auseinandersetzen müssen, können sie mehr Zeit in die Schulung und das Coaching anderer Mitarbeiter investieren und so auch die eigene Weiterentwicklung und Karriere vorantreiben.

Ein stärkeres Unternehmenswachstum

Sicherheitsexperten, die ihre eigenen Aufgaben effizient durchführen, können diese Fähigkeit auch dafür nutzen, Wachstumschancen für ihr Unternehmen im Zuge einer intelligenteren Datennutzung zu ermitteln (bzw. Abläufe auszumachen, die das Unternehmenswachstum bremsen könnten).

Bahn frei für die digitale Transformation

Wenn die Untersuchung datenschutzrelevanter Vorfälle im Gesamtkontext erfolgt und dadurch optimiert wird, verschafft dies den verantwortlichen Teams Zeit, Richtlinien und Verfahren so anzupassen, dass sie einer Cloud-basierten Datenkultur gerecht werden. Dies beschleunigt wiederum die digitale Transformation und bringt dem Unternehmen einen Wettbewerbsvorteil.

Daten in jedem Arbeitsumfeld schützen

Herkömmliche Maßnahmen zur Data Loss Prevention schützen Daten an drei Zugriffspunkten: in Ihrem Netzwerk, an Endpunkten und zunehmend auch in der Cloud. Diese Maßnahmen wären möglicherweise ausreichend, wenn sich alle Personen, die auf die betreffenden Daten zugreifen, ausschließlich innerhalb dieses Bereichs bewegten. In zunehmendem Maße ist allerdings das Überschreiten dieser Grenzen erforderlich, wodurch die bisherigen Maßnahmen für den Datenschutz nicht mehr ausreichen. Wie können also die neuen Anforderungen erfüllt werden?

Folgen der Cloud-Transformation

In Bezug auf die Cloud-Migration lautet die Frage nicht „ob überhaupt", sondern „wann". Die Anforderungen von mobilen Mitarbeitern, Kunden und strategischen Partnern beschleunigen diese Entwicklung noch und machen eine zeitnahe Umstellung auf die Cloud zu einem Muss. Beispiel: 87 % aller Unternehmen erwarten inzwischen von ihren Mitarbeitern, das persönliche Smartphone für mobile Geschäftsanwendungen zu nutzen.[3] Dieses Konzept ist weithin als „Bring Your Own Device" (BYOD) bekannt. Außerdem gibt fast ein Viertel aller Mitarbeiter der Generation Y an, bereits Unternehmensdateien auf diese Geräte heruntergeladen oder Cloud-Anwendungen anderer Anbieter („Bring Your Own Cloud", BYOC) installiert zu haben, ohne die IT-Abteilung oder Unternehmensleitung darüber in Kenntnis zu setzen. Daraus ergibt sich eine sogenannte Schatten-IT, was wiederum bedeutet, dass ein Unternehmen nicht immer die Kontrolle darüber hat, wann und wie es in die Cloud wechselt. Doch unabhängig vom Tempo der Entwicklung kann man die bisherigen Sicherheitsrichtlinien nur schwer an die neuen Anforderungen anpassen.

Grund dafür ist u. a., dass Anbieter von Cloud-Anwendungen in der Regel die Übertragbarkeit, Erreichbarkeit und Benutzerfreundlichkeit der Anwendung in den Vordergrund stellen. Diese drei Faktoren sollten jedoch auch für die Datensicherheit gelten. Meist besteht lediglich ein Konzept der gemeinsamen Sicherheitsverantwortung zum Schutz der Infrastruktur. Die Sicherheit der Daten innerhalb dieser Infrastruktur liegt aber weiterhin in der Verantwortung des Kunden. Das Arbeitsumfeld von heute befindet sich ständig im Fluss und Sie sind dafür verantwortlich, Datenschutzmaßnahmen zu etablieren, die unabhängig vom Standort Ihrer Mitarbeiter gelten.

Ab jetzt bestimmen die Mitarbeiter die Grenzen

Wie können Sie Daten schützen, die außerhalb Ihres Unternehmensnetzwerk genutzt werden? Denken Sie in neuen Dimensionen und konzentrieren Sie sich auf die Mitarbeiter.

Nur wenn der Datenschutz peronenbezogen ausgerichtet ist, kann unabhängig vom Arbeitsplatz eine sichere Umgebung für Daten geschaffen werden. Wird die Datensicherheit mit der Identität einer Person verknüpft, kann in den Richtlinien durch Erkennung der Absicht außerdem die persönliche Risikostufe berücksichtigt werden. Ist zum Beispiel ein langjähriger, vertrauenswürdiger Mitarbeiter in einen Vorfall involviert, kann das Risiko als geringer eingestuft werden als bei einem dubiosen Anbieter oder einem verärgerten ehemaligen Mitarbeiter. Die Überwachung der Datensicherheit auf menschlicher Ebene gibt zudem Aufschluss über die unterschiedlichen Geräte und Anwendungen, die für die Nutzung der Daten eingesetzt werden. Vor diesem Hintergrund können die Sicherheitsteams Bedrohungen besser erkennen und aus der Erfahrung lernen.

Der Business Case Datenschutz

Den Datenschutz auf die Mitarbeiter auszurichten ist eine gute Antwort auf die dynamische Realität von Unternehmen in der heutigen Zeit. Was ist der Mehrwert für Ihr Unternehmen? Für die Beantwortung dieser Frage muss zunächst ein Mythos entkräftet werden, der Sicherheitsteams die Arbeit erschwert: Schutz sei nicht mit Produktivität vereinbar. Mit den richtigen Tools und Prozessen können beide Faktoren voneinander profitieren.

Zielgerichtete Antworten

Bisher war das Blockieren riskanter Aktionen der gängige Weg, um Datenverluste zu verhindern, z. B. das Speichern einer sensiblen Unternehmensdatei auf einem persönlichen USB-Stick. Geht eine solche Aktion von einem verärgerten ehemaligen Mitarbeiter oder einem kurzzeitigen Vertragspartner aus, ist dieses Vorgehen durchaus sinnvoll. In den meisten Fällen gibt es jedoch eine harmlose Erklärung, wenn z. B. eine Führungskraft eine wichtige Datei lediglich sichern oder auf einen anderen Computer übertragen möchte. Da herkömmliche Sicherheitsrichtlinien den Unterschied nicht erkennen können, werden harmlose Cyber-Aktivitäten häufig routinemäßig blockiert, was die Produktivität des Unternehmens einschränkt.

Werden Risiken auf menschlicher Ebene bewertet, können auch Kontext und Intention berücksichtigt werden – weg von der pauschalen und hin zur zielgerichteten Sicherheitsstrategie. So werden die Arbeitsabläufe der Mitarbeiter seltener unterbrochen, und gleichzeitig haben die Sicherheitsteams einen geringeren Untersuchungsaufwand. Fortschritt wird nicht mehr ausgebremst, sondern gefördert.

Weniger Schwachstellen

Mitarbeiter, die keinerlei böse Absichten hegen, werden in ihrer täglichen Arbeit durch pauschale Sicherheitsrichtlinien ausgebremst – das führt zu Frustration. Um das Problem zu lösen, suchen sie u. U. (weiterhin ohne böse Absicht) nach einer Möglichkeit, die Sicherheitsmaßnahmen zu umgehen. So könnte man die Datei im oben genannten Beispiel in kleinere Segmente aufteilen, um sie per E-Mail an den eigenen Computer zu senden und über diese Zwischenstation doch noch auf dem USB-Stick speichern zu können.

Dadurch entstehen allerdings zwei Probleme: Erstens könnte das System eine solche Abfolge von Aktionen als noch bedrohlicher einstufen als den ursprünglichen Versuch, die Datei auf einem USB-Stick zu speichern, weil ein Versuch zur Umgehung der Sicherheitsmaßnahmen erkannt wird. Für die Untersuchung sind Zeit und Ressourcen erforderlich. Was allerdings deutlich schwerer wiegt: So arglos die Absicht auch sein mag – solche Aktionen schaffen neue Sicherheitslücken, die ausgerechnet die Sicherheitsrichtlinien untergraben, die auf sie aufmerksam gemacht haben. Wäre der Datenschutz personenbezogen ausgerichtet, könnte man flexibler und angemessener reagieren und die Abwärtsspirale stoppen, noch bevor sie beginnt.

Proaktive Strategie

Für Lehrkräfte, Haustierbesitzer und Datenschutzexperten ist es kein Geheimnis, dass es weitaus effizienter ist, Chaos von vornherein zu verhindern als es im Nachhinein zu beheben.

Wenn der Datenschutz personenbezogen ausgerichtet ist und Kontext und Verhaltensmuster in die Bewertung einfließen, können echte Gefahren ohne Beeinträchtigung des Tagesgeschäfts frühzeitig identifiziert werden. Mitarbeiter können ihrer Arbeit nachgehen und werden nicht von unflexiblen Sicherheitsrichtlinien ausgebremst. In den zuständigen Abteilungen können datenschutzbezogene Warnungen nach Dringlichkeit sortiert und somit nach Priorität bearbeitet werden. So funktioniert Datensicherheit ohne Einschränkungen.

Der neue Standard im Bereich Datenschutz

Da sich Sicherheitsbedrohungen stetig verändern, müssen wir unsere

Denkweise entsprechend anpassen, um unsere Daten zu schützen – und dies beinhaltet die Erkenntnis, dass es sich hierbei um einen fortlaufenden Prozess handelt. Daher haben wir unsere Grundsätze für den Datenschutz an den Bedürfnissen der Zukunft ausgerichtet:

1. Datensicherheit präventiv statt reaktiv gestalten
Das reaktive Implementieren von Sicherheitsrichtlinien gehört der Vergangenheit an – in Zukunft sollen Datensicherheitsteams die Mitarbeiter ihres Unternehmens im sicheren Umgang mit Daten anleiten.

2. Das Resultat: eine flexible Risikobewertung, die sich an Veränderungen des Verhaltens und des von einer Person ausgehenden Risikos anpasst.

3. Umfassende Bewertung von Daten
Mit allen Daten im Blick, ob außerhalb Ihres Netzwerks, über Endpunkte hinaus oder in der Cloud, erhalten Sie kontextbezogene Hinweise zur Intention der Benutzer und können so geeignete Sicherheitsmaßnahmen ergreifen.

4. Einheitliche Sicherheitsrichtlinien für jede Umgebung
Die Datensicherheit am Menschen auszurichten bedeutet einen umfassenden Schutz Ihrer Daten unabhängig vom Speicherort oder vom Zugriffspunkt.

Sind Sie bereit, Ihre Datensicherheit ab sofort proaktiv zu gestalten?

› **Weitere Informationen finden Sie in unserem Flyer**
Datenschutz: 9 Schritte zum Erfolg.

1. IBM Marketing Cloud, „10 Key Marketing Trends for 2017" (10 wichtige Marketing-Trends für 2017)
2. Ponemon Institute, „U.S. Cost of a Data Breach Study", 2017 (Studie zu den Kosten von Datenschutzverletzungen in den USA)
3. Syntonic, „BYOD Usage in the Enterprise", 2016 (Einsatz von BYOD in Unternehmen)

Forcepoint

forcepoint.com/contact

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datenschutz und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die verhaltensbasierten Lösungen von Forcepoint passen sich in Echtzeit an das Nutzerverhalten an und ermöglichen Mitarbeitern einen sicheren Datenzugriff bei voller Produktivität. Forcepoint mit Sitz in Austin, Texas, schafft sichere, vertrauenswürdige Umgebungen für Tausende von Kunden weltweit.