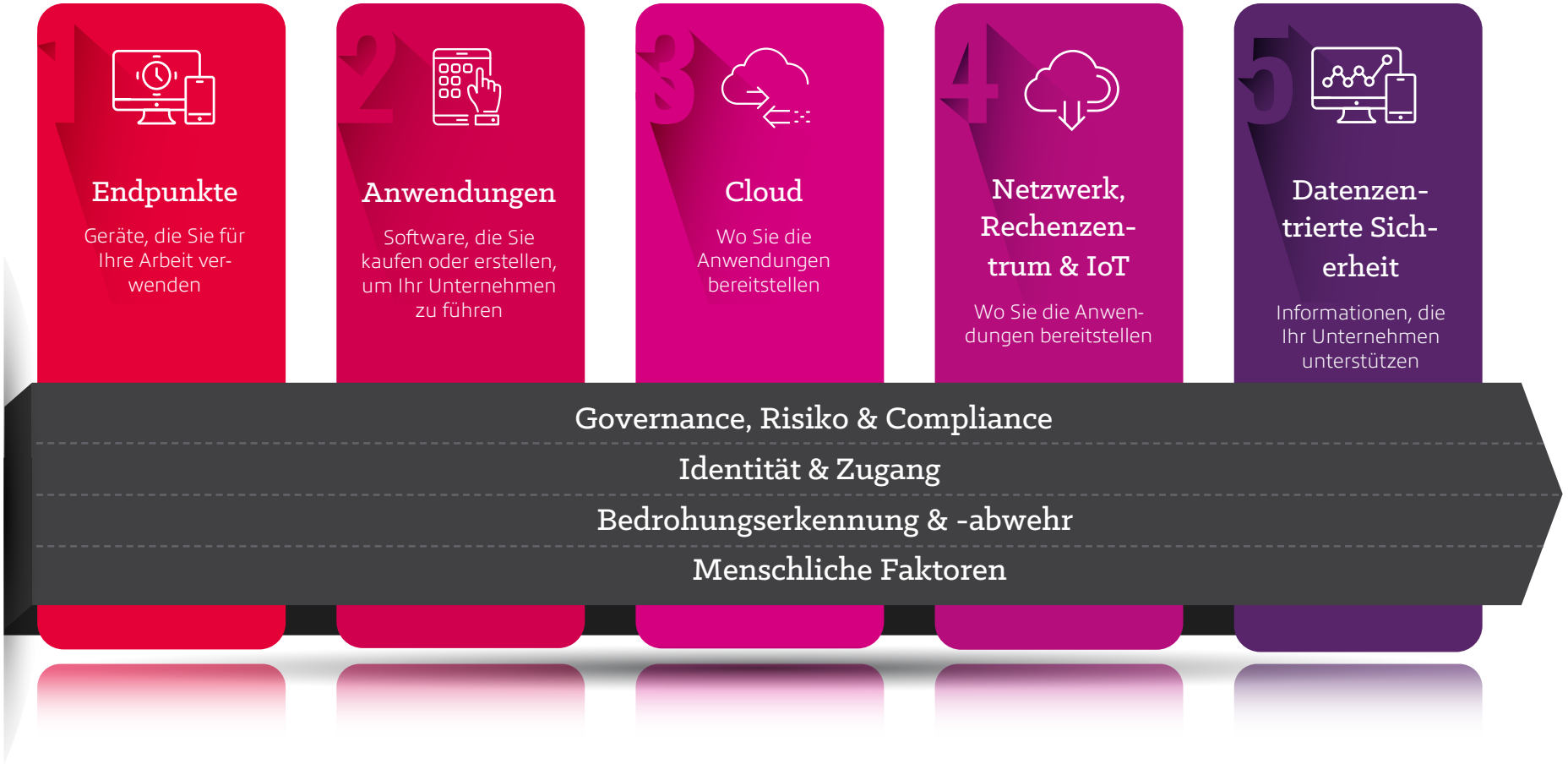
Insight

Leitfaden für datenzentrierte Sicherheit

Einführung

Wir bei Insight wissen, wie wichtig ein ganzheitlicher Ansatz für die IT-Sicherheit ist. Angreifer suchen nach Ihrem schwächsten Bereich, nicht nach Ihrem stärksten. Wir verfügen über technisches Fachwissen in den fünf Technologiebereichen (Endpunkte, Anwendungen, Cloud, Netzwerk, Rechenzentrum und IOT sowie datenzentrierte Sicherheit). Als führender Lösungsintegrator sind wir jedoch der Meinung, dass Sie auch den Wechselwirkungen zwischen diesen Technologiebereichen (Governance, Risiko und Compliance, Identität und Zugriff, Bedrohungserkennung und -abwehr sowie menschliche Faktoren) große Aufmerksamkeit schenken sollten. Die Lücken, in denen die Technologiedomänen miteinander verbunden sind, sind oft die Stellen, an denen ein zusätzlicher Nutzen erzielt werden kann, der dazu beiträgt, Ihre Gesamtsicherheit auf kostengünstige Weise zu verbessern.

Ganzheitliches Sicherheitsmodell



Was ist datenzentrierte Sicherheit?

Bei der datenzentrierten Sicherheit geht es um die Implementierung von Sicherheitskontrollen und -maßnahmen, die direkt die Daten selbst schützen und ihre Vertraulichkeit, Integrität und Verfügbarkeit gewährleisten. Ziel ist es, Daten im Ruhezustand, bei der Übertragung und der Nutzung zu schützen - unabhängig vom Speichermedium, der Netzinfrastruktur oder den beteiligten Anwendungen.

Die herkömmliche, auf dem Perimeter basierende Sicherheit ist nicht mehr ausreichend oder nachhaltig, wenn sich die meisten Personen, die auf die Daten zugreifen und diese nutzen, außerhalb des Unternehmensnetzwerks befinden.

Es gibt verschiedene Komponenten, die im Rahmen der dezentrierten Sicherheit zu beachten sind, und andere, die optional sind. Jedes Unternehmen hat seine eigenen individuellen Sicherheitsanforderungen. In diesem Leitfaden erläutern wir jede Komponente anhand unseres datenzentrischen Sicherheitsmodells.

Datenzentriertes Sicherheitsmodell

Wichtige Überlegungen im datenzentrierten Sicherheitsmodell

Sicherheitsexperten vebringen zwar viel Zeit mit der Sicherung von Anwendungen und Infrastrukturen, doch letztlich läuft fast alles, was wir tun, auf die Sicherung von Daten hinaus. Ob es sich nun um Mitarbeiterinformationen, Kundenaufträge, Produktionszahlen oder geistiges Eigentum handelt, es sind die Daten, die sich in Ihrem Unternehmen bewegen und die wahrscheinlich den größten Mehrwert für Ihre Endkunden und Ihr Unternehmen darstellen. Ein guter Ausgangspunkt für eine ganzheitliche Sicherheitsstrategie sind die Daten, und ein datenzentrierter Ansatz sollte mit den Interessengruppen Ihres Unternehmens und nicht mit der Technologie beginnen.

Datenverwaltung

Ein Zuviel an Sicherheit kann für Unternehmen ebenso schädlich sein wie ein Zuwenig, da es die Benutzer frustriert und die Geschäftsprozesse verlangsamt. Andererseits muss jede Organisation ein gesetzlich vorgeschriebenes Mindestsicherheitsniveau einhalten, wobei viele Branchen zusätzliche Schutzstufen verlangen, wie sie z.B. in PCI-DSS oder NIS2 vorgeschrieben sind. Die Abstimmung Ihrer Sicherheitsstrategie auf Ihre Geschäftsstrategie ist Teil des Managements Ihrer Datensicherheit und sollte die Grundlage für alle nachfolgenden technischen Entscheidungen sein.

Datenermittlung

Unternehmen haben im Laufe der Jahre riesige Datenmengen erzeugt, und diese werden in Zukunft noch zunehmen. Diese Daten können an verschiedenen Orten gespeichert sein, z.B. auf Servern vor Ort, in der Cloud und in verschiedenen Sicherungs- und Notfallwiederherstellungssystemen. Sie können in strukturierten Datenbanken organisiert sein oder in einem unstrukturierten Format in unkontrollierten Umgebungen wie Laptops existieren.

Für alles Weitere ist es entscheidend, einen Überblick darüber zu erhalten, welche Daten vorhanden sind und wo sie sich befinden - wir nennen dies Datenermittlung (Data Discovery). Es besteht die Tendenz, Daten länger als nötig aufzubewahren, nur für den Fall, dass sie verloren gehen, missbraucht oder gestohlen werden. Das Auffinden und die sichere Beseitigung dieser "veralteten" Daten kann sowohl Kosten als auch Risiko verringern und somit den Weg zur Datensicherheit vereinfachen.

Audit und Monitoring

Jetzt, da Sie wissen, wo sich Ihre Daten befinden, können Sie sicherstellen, dass jeder Zugriff darauf sowohl überwacht als auch geprüft wird. Ein minimales Maß an Auditing ist erforderlich, um zu sehen, wer die Daten wie nutzt, was nach einem Vorfall einen nützlichen Rückblick ermöglicht - nützlicher ist jedoch ein auf kontinuierlicher Überwachung basierender Ansatz für das Nutzerverhalten.

Verschiedene Techniken des maschinellen Lernens können angewandt werden, um ungewöhnliche Datenzugriffe außerhalb der üblichen Geschäftszeiten oder große Datenbewegungen zu erkennen, die auf einen potenziellen Verstoß hinweisen und es Ihnen ermöglichen, im Falle eines Vorfalls schneller zu reagieren.

Während viele Daten von Maschinen automatisiert verarbeitet werden, stellt die Nutzung der Daten durch Menschen das größte Risiko dar. Benutzer müssen keine böswilligen Absichten haben, um ein Risiko zu verursachen, sie können auch wohlmeinend sein und trotzdem Schaden anrichten.

Nutzer-Sensibilisierung und -Schulung

Die Sensibilisierung und Schulung der Benutzer wird oft übersehen, wenn es um Daten geht. Aber die Zeit, die im Vorfeld in diese Aktivitäten investiert wird, kann den Unterschied zwischen einer erfolgreichen oder einer gescheiterten Implementierung ausmachen.

Stellen Sie sich die Situation vor, dass ein Angestellter arbeitsbezogene Daten an eine private E-Mail-Adresse sendet, um nach Feierabend zu arbeiten. Dadurch entziehen sich die Daten der Kontrolle des Unternehmens. Um solche Probleme zu vermeiden, ist es wichtig, die Mitarbeiter im richtigen Umgang mit Daten zu schulen. Für den Erfolg jeder Datensicherheitsinitiative ist es außerdem wichtig zu verstehen, wie sich bevorstehende Änderungen auf die Geschäftsabläufe auswirken können.

Datenklassifizierung

Nicht alle Daten haben den gleichen Wert oder das gleiche Risiko und sollten daher nicht wie die Kronjuwelen behandelt werden. Als Teil Ihrer Data-Governance-Arbeit sollten Sie von Anfang an ein Datenklassifizierungsschema festlegen. Darin werden die allgemeinen Datenkategorien, mit denen Ihre Nutzer arbeiten werden, sowie die Art und Weise, wie die einzelnen Datentypen geschützt werden sollten, festlegen.

Jetzt ist es an der Zeit, Ihre Daten mit Sensibilitätskennzeichnungen zu versehen, die den Nutzern und verschiedenen automatischen Sicherheitskontrollen anzeigen, wie diese Daten behandelt werden sollten.

Verschlüsselung

Eine Möglichkeit, mit sensibleren Daten umzugehen, ist der Einsatz von Verschlüsselung. Dies ermöglicht eine genaue Kontrolle darüber, wer die Daten in ihrem ursprünglichen Format sehen und verwenden kann, was die Risiken verringert, wenn die Daten in die falschen Hände geraten, z.B. wenn ein Laptop gestohlen wird. Sie sollten eine Verschlüsselung für Daten in Erwägung ziehen, die sich im Ruhezustand befinden (auf Speichersystemen, die auf ihre Verwendung warten), in Bewegung sind (über ein Netzwerk fließen) oder gerade verwendet werden, d.h. vielleicht im Speicher gespeichert sind, während sie verarbeitet werden.

Maskierung

Die Maskierung ist eine weitere Kontrolle, die auf Daten angewandt werden kann, z.B. das Ausblenden der ersten 12 Ziffern einer Kreditkartennummer, wenn sie auf dem Bildschirm eines Callcenter-Mitarbeiters angezeigt wird.

Tokenisierung

Bei der Tokenisierung werden die eigentlichen sensiblen Werte durch einen eindeutigen, aber bedeutungslosen Wert in einer weniger sicheren Datenbank ersetzt, wobei die ursprünglichen sensiblen Daten an anderer Stelle in einem sichereren Bereich mit restriktiverem Zugang gespeichert werden.

Pseudonymisierung

Die Pseudonymisierung ähnelt der Tokenisierung, z.B. in Gerichtsakten, die der Öffentlichkeit zugänglich gemacht werden und in denen von "Zeuge 23" die Rede ist. Mit dem richtigen Zugang zum Daten-Mapping könnte der ursprüngliche Name wiedergefunden werden, aber für die meisten Zwecke kann die Privatsphäre gewahrt bleiben.

Anonymisierung

Die Anonymisierung ist ein weiterer Schritt, bei dem alle personenbezogenen Daten entfernt werden, so dass sie nicht mehr rückgängig gemacht werden können. Zum Beispiel könnte "12% der männlichen Patienten erlitten eine unerwünschte Reaktion auf ein Medikament" eine anonymisierte Zusammenfassung einer medizinischen Studie sein.

Backup und Recovery

Während sich Sicherheit oft auf die Vertraulichkeit (Datenschutz) und Integrität (Manipulationssicherheit) von Daten konzentriert, ist die Verfügbarkeit auch ein wichtiger Grundsatz der Sicherheit. Wenn kritische Daten nicht verfügbar sind, sei es aufgrund eines Hardware-Fehlers oder eines Ransomware-Angriffs, kann dies schwerwiegende Auswirkungen auf die Fähigkeit eines Unternehmens haben, zu arbeiten. Datensicherungs- und Wiederherstellungsverfahren sind erforderlich. Sie müssen gut definiert und getestet sein, um sicherzustellen, dass Daten zuverlässig innerhalb eines Zeitrahmens wiederhergestellt werden können. So dass der Geschäftsbetrieb fortgesetzt werden kann.

Aufbewahrung und Vernichtung

Ein wichtiger Bestandteil des Daten-Lebenszyklus ist die sichere Entsorgung von Daten, die nicht mehr benötigt werden. Dies kann Teil einer formellen Richtlinie zur Datenaufbewahrung sein, um Finanzdaten nach Ablauf der gesetzlich vorgeschriebenen Frist zu löschen oder Kundendaten auf GDPR-Antrag ("Recht auf Vergessenwerden") zu löschen. Es ist wichtig, Daten so zu löschen, dass sie nicht einfach wiederhergestellt werden können sowie die Sicherstellung, dass alle Kopien der Daten, einschließlich Backups, außerhalb der vernünftigen Nutzung liegen und ein Audit-Protokoll aufrecht-erhalten wird, ist dabei wichtig.

Zugangskontrolle

Eine wichtige Überlegung, die außerhalb der Datensicherheit liegt, aber für sie von entscheidender Bedeutung ist, betrifft die Identität. Identität ermöglicht Zugangskontrollen, bei denen Daten nur für die Personen oder Systeme zugänglich sind, die dazu autorisiert sind, sie anzuzeigen. Rollenbasierte Zugriffskontrolle ermöglicht granulare Einschränkungen für Gruppen von Personen und gibt an, wie auf Daten zugegriffen werden darf, z.B. nur lesen, aber nicht schreiben.

Prävention von Datenschutzverletzungen

Die Prävention von Datenschutzverletzungen dient als Rückhalt für Daten, die außerhalb definierter Richtlinien verwendet werden. Beispiele hierfür sind das Senden vertraulicher Daten außerhalb der Unternehmensgrenzen oder die versehentliche Übertragung von Informationen von Kunde A an Kunde B. Die Prävention von Datenschutzverletzungen kann den Nutzer auf eine potenzielle Verletzung aufmerksam machen oder in vielen Fällen verhindern, dass die Aktion ausgeführt wird. Es sollte z.B. bei E-Mails, Webverkehr, Zugriff auf Cloud-Repositories sowie an Endpunkten berücksichtigt werden, um zu verhindern, dass Daten auf USB-Sticks kopiert werden.

Wie Insight helfen kann

Die Bewertung der Datensicherheitslage von Insight bietet einen umfassenden Überblick über die Datensicherheitslage Ihres Unternehmens und liefert klare, detaillierte Empfehlungen für effektive, umsetzbare Verbesserungen.

Unsere auf Daten und Sicherheit spezialisierten Experten bewerten Ihre aktuellen Datenschutz-, Governance- und Privacy-Maßnahmen, um Risiken zu identifizieren. Wir dokumentieren, wie gut Ihre derzeitige Datenhaltung es Ihnen ermöglicht, Ihre Daten in Ihren On-Premise-, Cloud- und Hybrid-/Multi-Cloud-Umgebungen zu klassifizieren, zu schützen und zu verwalten.

Indem wir Ihre Datenlage und bestehenden Datenkontrollen und -prozesse genau bestimmen, versetzen wir Sie in die Lage, die am besten geeigneten Pläne, Kontrollen und Prozesse für die Einhaltung der Datenschutzbestimmungen zu implementieren, um Ihre Investitionsrendite zu maximieren.

Im Anschluss an die Bewertung Ihrer Datensicherheitslage kann Insight Sie bei der Technologiebeschaffung, der Implementierung sowie der Einführung und dem Change Management einer speziell auf Ihre Bedürfnisse zugeschnittenen Datensicherheitslösung unterstützen.