Die Risiken von Cyber-Bedrohungen – ein Leitfaden für CEOs und Vorstände

Ein Referenzmodell für IT-Sicherheitsexperten

Von:
Christopher Petersen
CTO & Mitbegründer von LogRhythm

Mit einem Vorwort von:
Sameer Bhalotra
Ehemaliger Sicherheitschef des Weißen Hauses

ES IST AN DER ZEIT, dass CEOs und Vorstände die Verantwortung übernehmen, die Cyber-Sicherheit in ihren Unternehmen zu verbessern. Globale Zahlungssysteme, Daten von Privatkunden, wichtige Überwachungssysteme und geistiges Eigentum – heute ist nichts mehr sicher vor Bedrohungen. Cyber-Kriminelle gehen immer intelligenter vor. Aufsichtsbehörden, Prozessanwälte und Gerichte beschäftigen sich verstärkt mit der Cyber-Kriminalität, die Öffentlichkeit wird sich mehr und mehr der Cyber-Risiken bewusst. Das Management und Führungskräfte von Unternehmen müssen sich jetzt dieser Herausforderung stellen.

Sameer Bhalotra

Ehemaliger Sicherheitschef des Weißen Hauses

Einführung

Einer der größten Händler Nordamerikas wurde ausgerechnet in der Einkaufszeit vor Weihnachten im Jahr 2013 Opfer eines Datendiebstahls im großen Stil. Cyber-Diebe manipulierten die Point-of-Sale-Systeme (POS-Systeme) und gelangten so an die Daten von 40 Millionen Kunden sowie an die persönlichen Daten von weiteren 70 Millionen Kunden.[1] Was die Menge an sensiblen Daten betrifft, die in Zusammenhang mit diesem Vorfall gestohlen wurden, handelt es sich um einen der größten Datendiebstähle der Geschichte.

Die Folgen dieses Vorfalls traten unmittelbar zu Tage und waren ernüchternd. Nach Bekanntgabe des Datendiebstahls brachen die Aktienwerte des Unternehmens um 11 % ein. Bei den Verkäufen wurde ein Minus von 3,8 % verzeichnet, da die Transaktionen während des wichtigen Weihnachtsgeschäfts um 5,5 % rückläufig waren.[2] Die Erträge im ersten Quartal 2014 gingen um 16 % zurück.[3] Bis zum zweiten Quartal 2014 verzeichnete das Unternehmen Ausgaben in Zusammenhang mit dem Datendiebstahl von 129 Millionen US- Dollar (netto) bzw. 13 US-Cent pro Aktie – und das war nur der Anfang.[4] Selbst heute noch steigen die Kosten, da sich das Unternehmen auf Sammelklagen und andere Klagen vorbereitet und gleichzeitig für die Finanzüberwachung für Tausende von Kunden aufkommt.

CEOs müssen die Cyber-Sicherheit ganz oben auf ihre Agenda setzen und sich damit auseinandersetzen, welches Risiko für ihr Unternehmen akzeptabel ist.

Der Datendiebstahl und der daraus resultierende Vertrauensverlust wirkten sich auch auf die Führungsriege des Unternehmens aus. Der CIO trat drei Monate nach Bekanntgabe des Datendiebstahls von seinem Amt zurück und der CEO verlor drei Monate später seinen Job – nicht zuletzt wegen der verheerenden Folgen des Datendiebstahls. Die ISS (Institutional Shareholder Services) empfahl den Aktionären, die Vorstände abzuwählen, die im Prüfungs- und Corporate Responsibility-Ausschuss tätig waren, da laut ISS das mangelhafte Risiko-Management der Ausschussmitglieder die Weichen für den Datendiebstahl stellte, der zu erheblichen Verlusten für das Unternehmen und die Aktionäre führte.[5]

Die Folgen des Datendiebstahls reichen weit über das betroffene Unternehmen hinaus. Banken und Kreditunternehmen haben bisher über 200 Millionen US-Dollar ausgegeben, um die Kredit- und EC-Karten der Kunden auszutauschen, die von dem Vorfall betroffen waren. Dieser eine Datendiebstahl betraf 10 % der EC- und Kreditkartenkunden aller Banken und Kreditkartenunternehmen in den USA.[6] Dabei sind die Konsumenten nicht direkt verantwortlich für finanzielle Verluste, die durch den Betrug in Zusammenhang mit diesem Datendiebstahl entstehen. Es ist jedoch zu erwarten, dass die Finanzinstitutionen, die normalerweise für Kreditkartenbetrug aufkommen, den betroffenen Händler verklagen werden, um die Kosten in Zusammenhang mit dem Datendiebstahl einzuklagen.

Neben diesem Einzelfall haben Cyber-Angriffe und Sicherheitsverletzungen bei einigen der größten Finanzinstitutionen der USA auf höchster Regierungsebene Aufmerksamkeit erregt. Präsident Obama und seine führenden Berater für die nationale Sicherheit wurden über Cyber-Angriffe auf JP Morgan Chase und neun weitere Finanzinstitute informiert. Es ist davon auszugehen, dass die Unternehmensführungen dieser Finanzinstitute mit der Regierung der USA zusammenarbeiten werden. Der Geheimdienst prüft die Details zu diesen Sicherheitsverletzungen, um die Drahtzieher und ihre Motive aufzudecken.

Diese und andere Angriffe, die die Schlagzeilen der Wirtschaftsnachrichten beherrschen, zeigen, dass die Einbeziehung von CEOs und Vorständen in die IT-Sicherheit unerlässlich ist. CEOs müssen Cyber-Sicherheit ganz oben auf ihre Agenda setzen und sich damit auseinandersetzen, welches Risiko für sie akzeptabel ist. Die IT-Sicherheit eines Unternehmens ist zu wichtig, um sie voll und ganz dem CIO und CISO zu überlassen und die Führungsebene gänzlich davon auszunehmen. Ein ernstzunehmender Cyber-Angriff kann schwerwiegende Folgen für die finanzielle Stabilität eines Unternehmens haben. Cyber-Angriffe sind als hohes Geschäftsrisiko zu betrachten, das besondere Aufmerksamkeit von CEOs und Vorständen erfordert.

[1] Brian Krebs, „The Target breach, by the numbers", 14. Mai 2014
[2] Paul Ziobro, „Target Earnings Slide 46 % After Data Breach", The Wall Street Journal, aktualisiert am 26. Februar 2014
[3] James Covert, „Target data crisis haunts Q1 earnings, with 16 % drop", New York Post, 21. Mai 2014
[4] Pressemitteilung, „Target Reports Second Quarter 2014 Earnings", 20. August 2014
[5] Paul Ziobro, „ISS urges overhaul of Target board after data breach", The Wall Street Journal, 28. Mai 2014
[6] Brief an den US-Senat von William Hughes, Senior Vice President für Staatsangelegenheiten beim Einzelhandelsverband, 3. Februar 2014

Ein wichtiger Schritt der Unternehmensführung ist es beispielsweise, das Budget, das für strategische Sicherheitsmaßnahmen eingeplant ist, in Cyber-Sicherheit zu investieren, um die ausgefeilten Angriffe der heutigen Zeit zu bekämpfen. Die Analysten von Gartner empfehlen eine Neugewichtung des Cyber-Sicherheitsbudgets, wobei große Beträge von reinen Präventionsmaßnahmen abgezogen, und in das Aufspüren von Bedrohungen und die Problembehebung investiert werden sollen.

Neil MacDonald, Vizepräsident und renommierter Analyst sowie emeritierter Mitarbeiter der Gartner Inc., schrieb Folgendes: „2020 können wir damit rechnen, dass Unternehmenssysteme permanent einer Gefährdung ausgesetzt sein werden. Sie werden nicht mehr verhindern können, dass Kriminelle mit ausgeklügelten und zielgerichteten Methoden in ihre Systeme eindringen. Leider konzentrieren sich die meisten Unternehmen bei ihren Ausgaben für Datensicherheit derzeit auf Vorbeugung, auf den fehlgeleiteten Versuch, alle Angriffe abzuwehren." Er ergänzt weiter: „Wir sind davon überzeugt, dass der größte Teil der Ausgaben für Datensicherheit zukünftig für die schnelle Erkennung und Reaktion aufgewendet werden wird, und in diesem Zusammenhang auch für Abwehrsysteme, die eine weitere Ausbreitung von Angriffen verhindern." Der Bericht von MacDonald enthält eine besonders wichtige Empfehlung: „Investieren Sie in Ihre Ressourcen zur Reaktion auf Angriffe. Entwickeln Sie einen Prozess, mit dem Sie schnell die Tragweite und die Auswirkung eines erkannten Eindringens erkennen können, und sorgen Sie für die entsprechende personelle Ausstattung."[7]

Security Intelligence – die Zielsetzungen

Kehren wir zurück zum Datendiebstahl bei einem großen Händler im Jahr 2013. Nachdem der Vorfall aufgedeckt wurde (wohlbemerkt von externen Quellen), begannen wochenlange ausführliche forensische Untersuchungen zu den Auslösern des Datendiebstahls. Die wahrscheinlich erstaunlichste Enthüllung war, dass das Unternehmen bereits vor dem katastrophalen Diebstahl sensibler Daten digitale Warnungen erhielt, dass am POS-System etwas nicht stimmte. Nur wenige Monate zuvor hatte der Händler ein 1,6 Millionen teures System zum Aufspüren von Malware installiert, das diverse Male korrekt verdächtige Aktivitäten erkannte und meldete. Das Unternehmen reagierte jedoch nicht angemessen auf diese Sicherheitswarnungen.[8]

Vor dem katastrophalen Diebstahl sensibler Daten erhielt das Unternehmen bereits digitale Warnungen, dass etwas nicht stimmte.

Man geht davon aus, dass Wochen vor dem Angriff auf die POS-Systeme die Anmeldedaten eines Klimaanlagenverkäufers gestohlen wurden. Diese Anmeldedaten wurden verwendet, um Zugriff auf die IT-Umgebung zu erhalten. So konnten die Cyber-Angreifer Daten ausspionieren und ihren Angriff vorbereiten.

Wäre das Unternehmen auf die gestohlenen Anmeldedaten, die darauf folgende interne Spionage oder letztendlich die Installation von Malware auf den POS-Systemen aufmerksam geworden, hätte der Datendiebstahl verhindert werden können. Das Unternehmen übersah jedoch frühe Anzeichen und ignorierte darauf folgende Warnsignale. Es stellt sich natürlich die Frage, weshalb der Händler nicht auf die Warnsignale reagierte. Das Unternehmen bestätigte selbst, dass die Frühwarnsignale falsch interpretiert worden waren.

Wenn es nicht ausreicht, Daten bestehender Sicherheitssysteme zu erfassen, diese in einem einzigen Repository zu speichern und wiederholt geschulten Sicherheitsmitarbeitern Warnmeldungen zu übermitteln, um Sicherheitslücken aufzudecken, ihnen vorzubeugen oder sie zumindest zu schließen, dann stellt sich die Frage, was erforderlich ist, um diese Aufgabe zu erfüllen. Jede Organisation, deren Aufgabe es ist, die Daten ihrer Kunden zu schützen, ihr geistiges Eigentum, ihre Geschäftsgeheimnisse und -strategien und damit letztendlich ihren Marktwert, ist mit dieser Frage konfrontiert.

[7] Neil MacDonald, Gartner, Inc., „Prevention is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence", 30. Mai 2013

[8] Michael Riley, Ben Elgin, Dune Lawrence und Carol Matlack, „Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It", Bloomberg Businessweek, 13. März 2014

Gefährliche Bedrohungen aufdecken

Praktisch jedes Unternehmen – ob Personen- oder Kapitalgesellschaft, klein, mittelständisch oder groß und ganz gleich in welcher Branche – ist heute Cyber-Angriffen auf breiter Basis ausgesetzt. Der Studie „Global State of Information Security Survey 2015" von PwC zufolge ist die Zahl erkannter Sicherheitsvorfälle seit 2009 im Durchschnitt jährlich um 66 % gestiegen. Die Befragungsteilnehmer bestätigten für 2014 insgesamt 42,8 Millionen erkannte Sicherheitsvorfälle. Dies bedeutet eine Steigerung von 48 % im Vergleich zum Vorjahr. Das entspricht 117.339 Angriffen pro Tag und zwar tagtäglich. Und das sind nur die erkannten und gemeldeten Vorfälle. Ein Unternehmen für Internetsicherheit gab kürzlich die Schätzung ab, dass bis zu 71 % aller Verstöße unerkannt bleiben.[9] Das Problem ist inzwischen so akut, dass über die Hälfte der US-amerikanischen Unternehmen die Bedrohung durch Internetkriminelle als eines ihrer drei größten Geschäftsrisiken einschätzt.[10]

Unternehmen müssen Transparenz schaffen und sich auf die Bedrohungen konzentrieren, die ein materielles Risiko darstellen und die eine unmittelbare Reaktion erfordern.

Die Sicherheitslösungen in den meisten Unternehmen liefern einen Strom an Informationen zu Ereignissen, die eine Bedrohung darstellen könnten. Hierzu zählen beispielsweise Verhaltensmuster in den Netzwerkaktivitäten, die den üblichen Prozessen nicht zu entsprechen scheinen. Die meisten Unternehmen haben in Erkennungstechnologien und Detektionsverfahren investiert, die Tausende bedrohlicher Ereignisse pro Stunde – in Großunternehmen sogar pro Minute – aufdecken. Dieser nie abreißende Strom an Daten schafft mehr Verwirrung als Klarheit. Dies macht es für die meisten Sicherheitsverantwortlichen schwer, wenn nicht sogar unmöglich, zu erkennen, welche der zugrunde liegenden Bedrohungen tatsächliche Risiken darstellen und genauer untersucht werden müssen. Zudem können manche Bedrohungen durch traditionelle Sicherheitssysteme gar nicht erkannt werden und erfordern einen völlig anderen Ansatz – und das erschwert die Lage zusätzlich. Unternehmen müssen Transparenz schaffen und sich auf die Bedrohungen konzentrieren, die ein materielles Risiko darstellen und die eine unmittelbare Reaktion erfordern.

Genau dies ist die Aufgabe von Security Intelligence. Business Intelligence hilft Unternehmen dabei, in riesigen Mengen an Geschäftsdaten bislang ungenutzte Chancen zu entdecken und diese in Wettbewerbsvorteile zu verwandeln. Security Intelligence leistet Ähnliches für Bedrohungsdaten und ermöglicht es Unternehmen, ernstzunehmende Bedrohungen klar zu erkennen, damit sie Risiken schnell und effizient minimieren können. Die wichtigste Zielsetzung von Security Intelligence ist es, die richtigen Daten zum richtigen Zeitpunkt im passenden Kontext bereitzustellen, um den Zeitaufwand für die Erkennung und Reaktion auf Cyber-Bedrohungen deutlich zu verkürzen.

[9] PwC, „The Global State of Information Security Survey 2015", www.pwc.com/gsiss2015

[10] BAE Systems, „Business and the Cyber Threat: The Rise of Digital Criminality", Februar 2014

Reaktion auf Bedrohungen

Eine effektive IT-Sicherheit erfordert kompetente Mitarbeiter, klar definierte Richtlinien und Prozesse sowie eine Palette integrierter Technologien. Sowohl die Zahl der Cyber-Bedrohungen als auch die Raffinesse der Angriffsmethoden wächst stetig. Daher ist die Sicherheitstechnologie entscheidend, um in Verbindung mit dem Fachwissen der Mitarbeiter potenziell schädliche Bedrohungen erfolgreich zu erkennen und darauf zu reagieren.

Hinweise auf Cyber-Bedrohungen finden sich in den zugrunde liegenden forensischen Daten. Forensische Daten bestehen aus den Protokoll- und Maschinendaten, die kontinuierlich von jedem Server und Gerät, jeder Anwendung und Datenbank sowie jedem Sicherheitssystem in der gesamten IT-Umgebung erstellt werden. Zusätzliche Transparenz schafft der gezielte Einsatz forensischer Sensoren, die tief greifende Einblicke in Server, Endpunkte und Netzwerke eröffnen. In dieser riesigen Datenmenge finden sich klare Anhaltspunkte für Bedrohungen. Die Rolle von Security Intelligence ist es, die in diesen Daten enthaltenen Erkenntnisse herauszustellen, um Organisationen dabei zu unterstützen, diejenigen Bedrohungen, die für Schaden sorgen könnten und ein tatsächliches Risiko darstellen, zuverlässig zu ermitteln und eine durchgängige Erkennung von Bedrohungen und Reaktion darauf (End-to-End Threat Detection and Response™) zu ermöglichen.

Unternehmen, die ihren Sicherheitsstatus verbessern möchten, müssen in einen stabilen und weitgehend automatisierten, durchgängigen Prozess für die Erkennung von Bedrohungen und die Reaktion darauf investieren. Dieser Prozess kann als Abfolge verschiedener Phasen beschrieben werden:

Abbildung 1: Der End-to-End-Lebenszyklus von der Bedrohungserkennung bis zur Reaktion darauf

Im Rahmen des durchgängigen Prozesses zur Erkennung von Bedrohungen und der Reaktion darauf gibt es zwei wichtige Metriken, die Organisationen messen und optimieren sollten: die Mean-Time-to-Detect™ (mittlere Zeit bis zur Entdeckung, MTTD™) sowie die Mean-Time-to-Respond™ (mittlere Zeit bis zur Reaktion, MTTR™).

- Die MTTD ist der durchschnittliche Zeitbedarf, der benötigt wird, um diejenigen Bedrohungen zu entdecken und einzustufen, die der Organisation potenziell Schaden zufügen könnten.
- Die MTTR ist der durchschnittliche Zeitbedarf, den das Unternehmen benötigt, um die Bedrohung eingehend zu untersuchen und eventuelle Risiken zu minimieren.

Unglücklicherweise werden MTTD und MTTR bei vielen Organisationen wochen- oder monatsweise erfasst. Verizon berichtete im Jahr 2013, dass 66 % der Sicherheitsprobleme, die im Rahmen einer jährlichen Studie untersucht wurden, erst nach Monaten oder Jahren entdeckt wurden. Sicherheitslücken, die von den betroffenen Unternehmen über Monate unentdeckt bleiben, ermöglichen es Angreifern, sich im Netzwerk des Unternehmens einzunisten und ihre bösartige Mission aufzunehmen und möglicherweise auch zum Abschluss zu bringen. Daher müssen Unternehmen, die ihre Cyber-Sicherheitsrisiken verringern möchten, ihre MTTD- und MTTR-Metriken mindestens auf Tages-, Stunden-, oder – im Optimalfall – auf Minutenbasis erheben. Wirkliche Fortschritte bei diesen Kennzahlen lassen sich jedoch nur durch Security Intelligence erzielen.

Sie beruht nicht auf einer einzelnen Technologie, sondern einer weitgehend integrierten Reihe von Technologien, die für die erforderliche forensische Transparenz sorgen und Sicherheitsteams dabei unterstützen, möglichst effizient Risiken zu ermitteln, einzustufen, zu untersuchen, zu minimieren und zu beseitigen. Ein einheitlicher Security-Intelligence-Ansatz stellt sicher, dass Technologie, Mitarbeiter und Prozesse präzise aufeinander abgestimmt sind und das Ziel verfolgen, MTTD, MTTR und letztendlich die Geschäftsrisiken zu vermindern.

Bewertung der Security-Intelligence-Reife einer Organisation

Führungskräfte müssen wissen, inwieweit ihr Unternehmen Sicherheitsbedrohungen abwehren und Risiken minimieren kann. Das LogRhythm Security-Intelligence-Maturity-Model™ (SIMM™) unterstützt Unternehmen dabei, anhand ihrer Security-Intelligence-Fähigkeiten und Organisationsmerkmale ein Verständnis für die Risiken zu entwickeln. Die Reifegrade erstrecken sich von Grad 0 für Unternehmen, die keinerlei Investitionen in Security-Intelligence-Funktionen getätigt haben und daher einem hohen Risiko erfolgreicher Cyber-Angriffe ausgesetzt sind, über Grad 1, bei dem minimalen Compliance-Anforderungen Rechnung getragen wird, zu Grad 2, bei dem das Unternehmen für die Einhaltung der Compliance-Vorgaben gut aufgestellt ist und über verbesserte Funktionen zur Reaktion auf Bedrohungen verfügt. Bei Grad 3 ist das Unternehmen aufmerksam bei der Suche nach Bedrohungen und reagiert meist schnell auf diese. Unternehmen mit Reifegrad 4 sind schließlich in der Lage, als entschlossener Gegner selbst schwersten Angriffen standzuhalten und sich gegen diese zu verteidigen.

(Eine Übersicht über das Security-Intelligence-Maturity-Modell finden Sie in Anhang A.)

Führungskräfte müssen wissen, inwieweit ihr Unternehmen Sicherheitsbedrohungen abwehren und Risiken minimieren kann.

Umsichtige Unternehmer versuchen, ihren Reifegrad im SIMM zu steigern, um ihren Sicherheitsstatus zu optimieren und Angriffe abzuwehren, die dem Unternehmen potenziell Schaden zufügen können. Der Aufstieg im Reifemodell hängt von den Erkennungs- und Reaktionsfähigkeiten ab, die auf Sicherheitstechnologien wie ganzheitliche Protokollverwaltung, Netzwerk- und Endpunktforensik, Verhaltens- und Korrelationsanalysen, Sicherheitsinformations- und Ereignis-Management (SIEM) und vielem mehr beruhen.
Unternehmen, die den höchsten Reifegrad im SIMM erreicht haben, weisen folgende Merkmale auf:

- Sie verfügen über äußerst robuste Prozesse und sind bei der Einhaltung gesetzlicher Vorschriften höchst effizient.
- Sie sind in der Lage, alle Klassen von Cyber-Bedrohungen zu entdecken und schnell darauf zu reagieren.
- Sie können Hinweise auf sehr raffinierte Bedrohungsarten (wie die sogenannten Advanced Persistent Threats oder APTs) schon in frühen Phasen des Angriffs erkennen und deren Aktivitäten eindämmen.
- Sie sind in der Lage, sich gegen Angriffe von Gegnern auf globaler Ebene zu schützen und zu verteidigen.

Je fortgeschrittener die Security Intelligence eines Unternehmens ist, desto geringer fallen MTTD und MTTR aus, wodurch wiederum das Risiko sinkt, einem schädlichen Cyber-Vorfall ausgeliefert zu sein. Natürlich muss jedes Unternehmen – basierend auf der jeweiligen Risikotoleranz – für sich selbst den passenden Reifegrad ermitteln, den es erreichen möchte.

Glücklicherweise können auch Unternehmen mit begrenztem Budget und höherer Risikotoleranz bereits deutliche Sicherheitsverbesserungen erreichen, wenn sie sich hin zu Reifegrad 2 entwickeln. Bei Organisationen, die größere Ressourcen auf die Cyber-Sicherheit verwenden können und deren Risikotoleranz deutlich niedriger liegt, können die Reifegrade 3 oder sogar 4 erstrebenswerte Ziele sein.

Dank der einheitlichen Plattform von LogRhythm und einer flexiblen Produktarchitektur können Unternehmen den Funktionsumfang bedarfsorientiert erweitern. Dabei können sie sich darauf verlassen, dass zukünftige Investitionen stets auf dem vorangegangenen Schritt im Maturity-Modell aufbauen. LogRhythms Ziel ist es, den Unternehmen ein Partner zu sein, der ihnen die integrierten technologischen Bausteine und zugehörigen Dienstleistungen liefert, mit denen sie in die Lage versetzt werden, ihre Security-Intelligence-Ziele zu erreichen und sich vor schädlichen Cyber-Bedrohungen zu schützen.

Fazit

CEOs und Vorstandsmitglieder von Unternehmen müssen Verantwortung übernehmen und sich mit IT-Sicherheit und den damit einhergehenden Geschäftsrisiken auseinandersetzen. Sie müssen wissen, wo ihr Unternehmen sich im Security-Intelligence-Maturity-Modell befindet. Sie müssen die Risikobereitschaft ihres Unternehmens sowie ihre Fähigkeiten zur Risikominimierung einschätzen können und dann ggf. einen Plan entwickeln, um vorhandene Lücken zu schließen. Das Security-Intelligence-Maturity-Modell von LogRhythm liefert eine wertvolle Orientierung, um die notwendigen Ebenen und Strukturen für die Erkennung von Bedrohungen und deren Abwehr aufsetzen zu können.

Über LogRhythm

LogRhythm, eines der führenden Unternehmen für Security Intelligence und Sicherheitsanalysen, unterstützt Unternehmen weltweit dabei, Cyber-Bedrohungen aufzuspüren sowie Probleme zu beheben. Die patentierte und preisgekrönte Plattform des Unternehmens vereint auf einzigartige Weise SIEM der nächsten Generation mit Protokollverwaltung, Netzwerk- und Endpunktforensik sowie fortschrittlichen Sicherheitsanalysen. LogRhythm schützt Kunden nicht nur vor den Risiken in Zusammenhang mit Cyber-Bedrohungen, sondern bietet darüber hinaus unübertroffene Automatisierung und Einhaltung der Compliance sowie der IT-Intelligence.

Die marktführende Rolle von LogRhythm spiegelt sich auch in vielen Auszeichnungen wider. Das Unternehmen nahm drei Jahre in Folge die Position eines „Leader“ im Magic Quadrant-Bericht von Gartner zum Thema SIEM ein, wurde im SIEM Vendor Landscape-Bericht 2014/15 der Info-Tech Research Group als „Champion“ ausgezeichnet und im SIEM Appliance Buyer's Guide von DCIG 2014/15 als „Best-in-Class“ (Nr. 1) eingestuft. Darüber hinaus erhielt LogRhythm den SIEM Global Market Penetration Leadership-Preis von Frost & Sullivan und wurde von der Denver Post als hervorragender Arbeitgeber ausgezeichnet.

Die vollständige Version dieses Dokuments mit dem Titel **Aufdecken kritischer Cyber-Bedrohungen durch Security Intelligence: *Ein Referenzmodell für IT-Sicherheitsexperten*** können Sie unter folgender Adresse herunterladen oder weiterleiten: www.logrhythm.com/SIMM-CISO

Anhang A

Übersicht über das Security-Intelligence-Maturity-Model von LogRhythm

Im nachfolgenden Diagramm sind die Security-Intelligence-Fähigkeiten eines Unternehmens nach Reifegrad zusammengefasst.

FUNKTION	BESCHREIBUNG	REIFEGRAD 0	REIFEGRAD 1	REIFEGRAD 2	REIFEGRAD 3	REIFEGRAD 4
	MTTD WIRD TYPISCHERWEISE GEMESSEN IN:	2015 JAHREN	MONATEN	TAGEN	STUNDEN	MINUTEN
	MTTR WIRD TYPISCHERWEISE GEMESSEN IN:	MONATEN	WOCHEN	TAGEN	STUNDEN	MINUTEN
SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)	Das Unternehmen hat SIEM eingeführt und nutzt Dashboards, Analysen, Berichte, Risikomanagement, Warnmeldungen sowie Incident Response-Maßnahmen und Automatisierungsfunktionen.	○	◔	◑	◕	●
LOG-DATEN-MANAGEMENT	Das Unternehmen nutzt eine Standardlösung für die Log-Daten-Verwaltung, die eine zentralisierte und sichere Erstellung eines forensischen Protokolls sowie das Abrufen von Maschinen- und Ereignisdaten ermöglicht.	○	◔	◕	●	●
SERVER-FORENSIK	Das Unternehmen nutzt Agents auf den Servern, um eine umfassende forensische Transparenz der Server-Aktivitäten zu erzielen. Dies umfasst unter anderem die Überwachung der Datenintegrität, der Verzeichnisse, der Prozessaktivitäten, der Netzwerkaktivitäten und vieles mehr.	○	◔	◕	●	●
ENDPUNKT-FORENSIK	Das Unternehmen nutzt Agents an den Endpunkten, um eine umfassende forensische Transparenz der Aktivitäten von Workstations und mobilen Geräten zu erzielen. Dies umfasst unter anderem die Überwachung der Datenintegrität, der Verzeichnisse, der Prozessaktivitäten, der Netzwerkaktivitäten und vieles mehr.	○	○	○	◑	●
NETZWERK-FORENSIK	Das Unternehmen nutzt Netzwerk-Forensiksensoren zur Überwachung interner und externer Netzwerkaktivitäten, sowie ein umfassendes Paketerfassungsprogramm.	○	○	○	◑	●
MASCHINENANALYSEN	Das Unternehmen nutzt eine automatische Echtzeitanalyse-technologie, die Log-Daten und Kontextinformationen dazu einsetzt, Bedrohungen aufzuspüren und zu priorisieren – anhand verschiedener Analyseansätze wie beispielsweise der erweiterten Korrelation und der Aufdeckung von Anomalien.	○	○	◑	◕	●
INFORMATIONEN ZU SCHWACHSTELLEN	Das Unternehmen prüft und bewertet die Umgebung aktiv auf mögliche Schwachstellen, die von einem Angreifer genutzt werden könnten. Diese Informationen werden für die Verbesserung der Analysen und der Sicherheit verwendet.	○	○	◔	◕	●
INFORMATIONEN ZU BEDROHUNGEN	Das Unternehmen nutzt Informationen zu Bedrohungen aus offenen Quellen, der Gemeinschaft und der Wirtschaft über verschiedene Bedrohungsvektoren hinweg. Die Informationen werden zur Verbesserung der Analysen und der Sicherheit verwendet.	○	○	◔	◕	●
ÜBERWACHUNG UND REAKTIONSMAßNAHMEN	Das Unternehmen hat Standardprozesse für die Überwachung und die Reaktion auf Bedrohungen und alle damit zusammen-hängenden Vorfälle eingeführt.	○	◔	◑	●	●
SECURITY OPERATIONS CENTER	Das Unternehmen hat ein Security Operations Center eingeführt, um eine Überwachung rund um die Uhr zu garantieren und globale Bedrohungsanalysen und Reaktionsmaßnahmen auf Vorfälle bereitzustellen.	○	○	○	◑	●

Fortsetzung auf Seite 9

Anhang A

Übersicht über das Security-Intelligence-Maturity-Model von LogRhythm *Fortsetzung*

Im nachfolgenden Diagramm sind die Risikomerkmale eines Unternehmens nach Reifegrad zusammengefasst.

RISIKOEINSTUFUNG	BESCHREIBUNG	REIFEGRAD 0	REIFEGRAD 1	REIFEGRAD 2	REIFEGRAD 3	REIFEGRAD 4
COMPLIANCE-RISIKO	Das Unternehmen ist in der Lage, problemlos und effizient sämtliche obligatorischen Compliance-Anforderungen zu erfüllen.	○	◑	●	●	●
RISIKO INTERNER BEDROHUNGEN	Das Unternehmen ist in der Lage, interne oder von internen Quellen ausgehende Bedrohungen in der geschützten internen Umgebung aufzuspüren und darauf zu reagieren.	○	◔	◑	●	●
RISIKO EXTERNER BEDROHUNGEN	Das Unternehmen ist in der Lage, externe Bedrohungen, die ihren Ursprung außerhalb der geschützten Umgebung haben, aufzuspüren und darauf zu reagieren.	○	◔	◕	●	●
RISIKO EINES ADVANCED PERSISTENT THREATS	Das Unternehmen ist in der Lage, Bedrohungen auf dem Niveau eines Advanced Persistent Threats aufzuspüren, darauf zu reagieren und sich so vor kriminellen, aktivistischen oder terroristischen Zielen zu schützen.	○	○	◔	◕	●
RISIKO EINER GLOBALEN BEDROHUNG	Das Unternehmen ist in der Lage, globale Bedrohungen aufzuspüren, darauf zu reagieren oder sich davor zu schützen.	○	○	○	◑	●

LogRhythm™
The Security Intelligence Company

LR_SIMM_CEO_01.15

LogRhythm™