IDC's Security Assessment Zusammenfassungsbericht

Kurzfassung

Vielen Dank für Ihre Teilnahme an der IDC-Umfrage zur Reaktionsbereitschaft bei Sicherheitsvorfällen, die von Splunk gesponsert wird. Dieses Tool will Unternehmen vergleichende Informationen zu ihrer Reaktionsbereitschaft bei Sicherheitsvorfällen liefern, die durch unabhängige Forschung untermauert werden. In der Umfrage wurden Antworten von Personen in 600 Unternehmen weltweit gesammelt, die Einfluss auf den Bereich der Sicherheit haben oder für das Budget verantwortlich sind. Sie sollen die Unterschiede aufzeichnen, die zwischen innovativen Unternehmen in Bezug auf Sicherheitsstrategie, die Vorfallserkennung und die Reaktion auf Vorfälle bestehen.

Basierend auf der Auswertung der einzelnen Antworten in dieser Umfrage hat IDC einen Vergleichsrahmen erstellt und die Unternehmen in fünf verschiedene Stufen der Reaktionsbereitschaft auf Sicherheitsvorfälle eingeteilt. Die Einteilung erfolgte je nach Herangehensweise der Unternehmen hinsichtlich Sicherheitsstrategien, Vorfallserkennung und Reaktion auf Vorfälle, siehe Abbildung 1. Vorteile ergeben sich für Unternehmen nicht erst am oberen Ende der Skala. Jede Verbesserung bringt greifbare Vorteile für die IT und das Unternehmen, da sie Flexibilität, Widerstandsfähigkeit und Innovation erhöht. Die Fähigkeit, die Strategie an wechselnde Marktbedingungen anzupassen, stärkt das Selbstvertrauen des Unternehmens.

Stufe 1: Schlecht

Risiko einer Sicherheitsverletzung wird nicht wahrgenommen.
Reaktiv.
Kein Vorfallsreaktionsplan.
Kein Vorfallsreaktionspartner.
Im Krisenmodus.
Weigerung, sich Risiken zu stellen.
Ressourcen bei der Vorfallsreaktion werden ungeplant und spontan abgestellt, zumeist aus internen Ressourcen.

Stufe 2: Normal

Beschränkte Ressourcen zur Auffindung von Sicherheitsproblemen.
Elementare Partnerschaftsbeziehung zur Vorfallsreaktion, aber spontan.
Ressourcen bei der Vorfallsreaktion werden geplant und zumeist aus internen Ressourcen abgestellt.
Intern entwickelte Lösungen/Verfahren zur Erkennung von Vorfällen.

Stufe 3: Gut

Anerkennung, dass Sicherheitsprobleme unvermeidbar sind.
Vorfallsreaktionspartner in Bereitschaft, mit im Voraus bezahlten Zeitblöcken.
Formeller Cyber-Bereitschaftsplan, der nicht oft getestet wird. Ressourcen zur Vorfallsreaktion sind geplant und bestehen aus einer Kombination interner und externer Ressourcen.
Grundlegende Analyse vorhanden, basierend auf Informationen aus SIEM-Feeds.
Gewisse Integration zwischen Sicherheitsprodukten, wahrscheinlich speziell angefertigt.
Gutes Verständnis der Risikosituation.

Stufe 4: Ambitioniert

Geht von Sicherheitsproblemen aus.
Verfügt über eine Reihe von Fachleuten zur Vorfallsreaktion, die bei einem Vorfall die nötigen Ressourcen und Fachkenntnisse zur Verfügung stellen können.
Formeller Bereitschaftsplan zur Vorfallsreaktion, der jährlich getestet wird.
Ressourcen bei der Vorfallsreaktion werden geplant und zumeist aus externen Ressourcen gestellt.
Standardisierte Vorfallsreaktionspläne basieren auf formellen Verfahren und Run-Books.

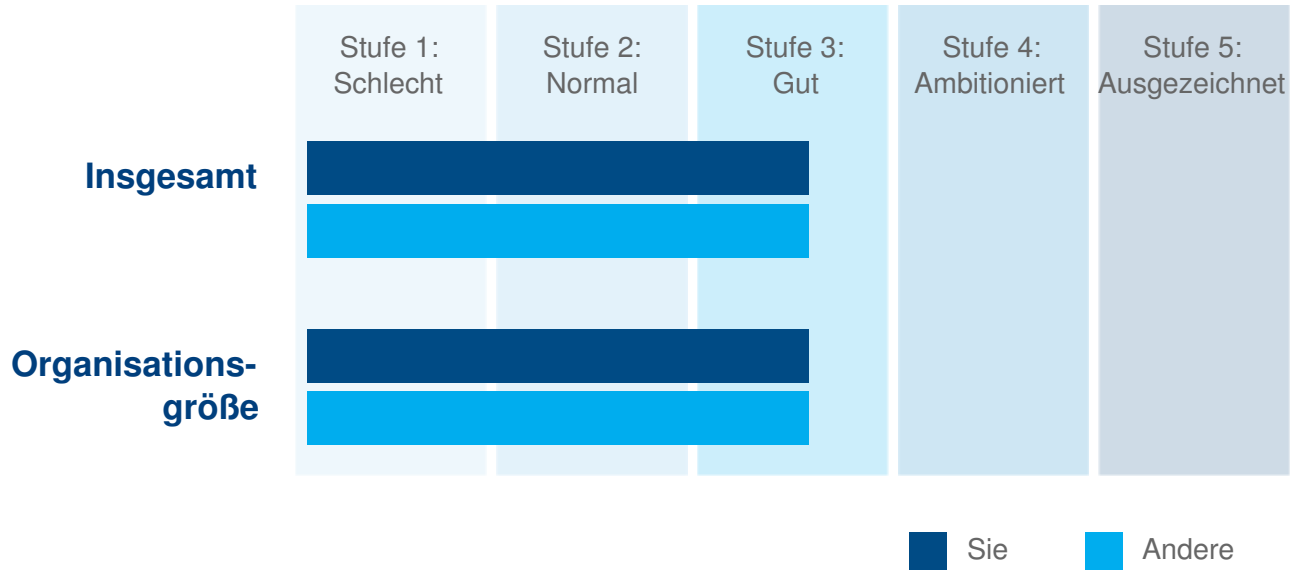
Stufe 5: Ausgezeichnet

Proaktive Aufspürung von Sicherheitsvorfällen.
Fokussiert auf Best Practices und kontinuierliche Verbesserung.
Vorfallsreaktionsplan vorhanden und regelmäßig getestet.
Permanentes Vorfallsreaktionsteam (im Haus oder unabhängiger Anbieter).
Rechtliche Vereinbarung zur Weitergabe von Vorfallsreaktionsdaten.
Ressourcen zur Vorfallsreaktion sind geplant und bestehen aus einer Kombination aus internen Mitarbeitern und temporär gebuchten externen Ressourcen, mit denen regelmäßige Planungstreffen abgehalten werden.
Einheitliche und integrierte Sicherheitsmanagementlösung für eine holistische Sicht der Sicherheitslage.
Risiko ist der treibende Faktor bei den Beurteilungs- und Minderungsverfahren.

Gesamtergebnis

Basierend auf Ihren Antworten wurden Sie mit **41**% der Unternehmen insgesamt in die Bereitschaftsgruppe **Stufe 3: Gut**, eingeordnet, d. h. Stufe **3rd** von insgesamt fünf Stufen.

ABBILDUNG 2: Ergebnis der IDC-Beurteilung zur Reaktionsbereitschaft bei Sicherheitsvorfällen



Gesamtübersicht

Im Vergleich mit Unternehmen mit ausgezeichneten Kompetenzen liegt Ihr Unternehmen:

- Inline with the global leaders
- Inline with the leaders in companies of the same size

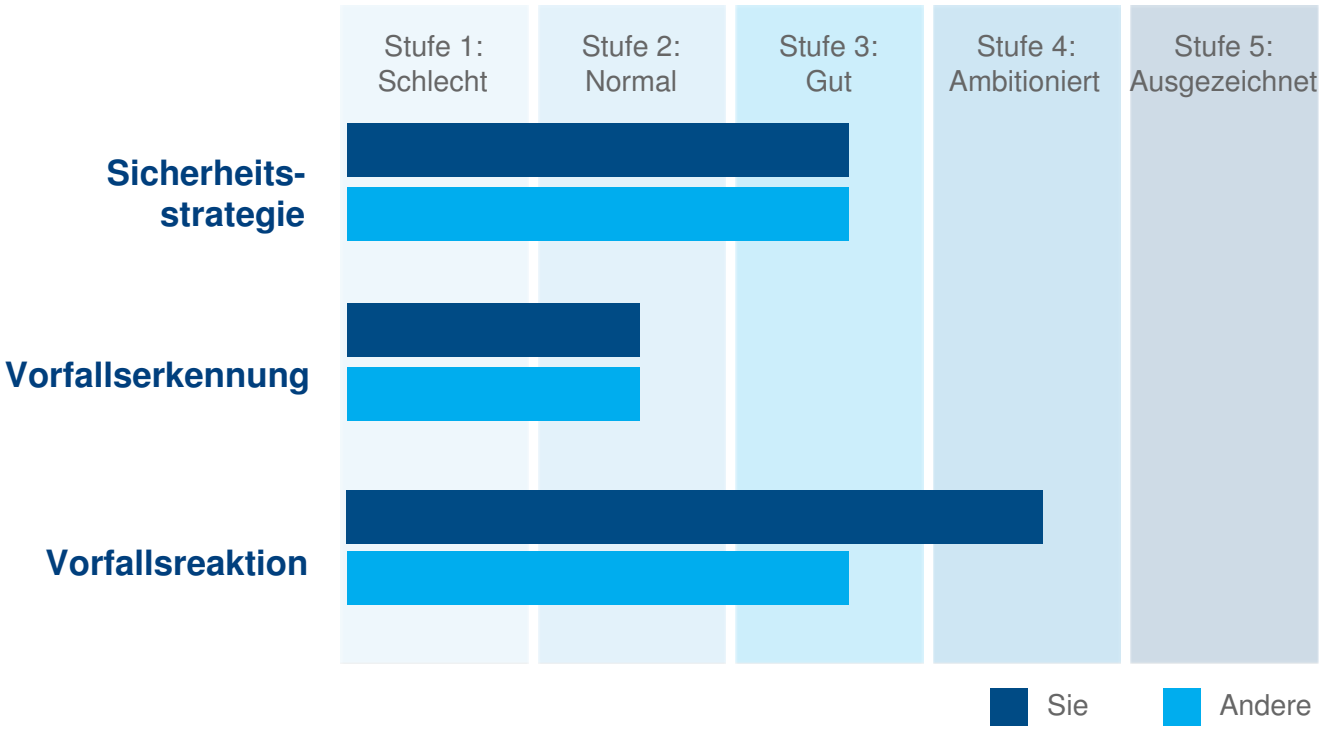
Ihre Performance im Detail
Dieses Beurteilungstool soll einschätzen, inwieweit Ihr Unternehmen heute und in Zukunft in der Lage ist, mit den steigenden Risiken umzugehen, denen sich digitale Unternehmen gegenübersehen.
Wir haben uns folgende Schlüsselbereiche der IT-Sicherheit angesehen:

- **Sicherheitsstrategie**
- **Vorfallserkennung**
- **Vorfallsreaktion**

Ihre Performance in den einzelnen Bereichen wird in Abbildung 3 mit ähnlichen Unternehmen verglichen.

IDC: Reaktionsbereitschaft bei Sicherheitsvorfällen nach Kompetenz

ABBILDUNG 3: IDC: Reaktionsbereitschaft bei Sicherheitsvorfällen nach Kompetenz



Welche Verbesserungsmaßnahmen wären sinnvoll?

Unabhängig von Ihrer Stufe gibt es einige Bereiche, die sich ständig weiterentwickeln und auf die Sie sich zuallererst konzentrieren sollten:

- Integration: Vermeiden Sie eine zentrale Ansicht.
- Proaktiver Ansatz: Reduzieren Sie die Zeit zwischen Sicherheitsvorfall und Erkennung von Monaten auf Stunden (oder noch weniger).
- Nase vorn bei der Compliance: Für die meisten Unternehmen ist es schwer genug, Compliance zu erreichen, geschweige denn, sie aufrecht zu erhalten.
- Best Practices: Seien Sie sich bewusst, dass sich das Risikoumfeld ständig ändert und dass Compliance und aufsichtsrechtliche Rahmenwerke oft schon bei der Einführung um Jahre veraltet sind. Best Practices sind der beste Weg, die Risiken zu mindern. Und ein zusätzlicher Vorteil ist, dass sich, wenn Sie diesen Ansatz richtig verfolgen, die Compliance von selbst einstellt.

Verbesserungen der Vorfallsreaktion

Das Management der ersten Reaktion auf einen Sicherheitsvorfall ist von entscheidender Bedeutung, wenn es gilt, das Risiko einzugrenzen und mögliche Schäden zu mindern. Bis jetzt fehlt Ihnen hier noch die nötige Planung. Eine Plattform, die diesen Bereich standardisiert und verwaltet, kann besonders nützlich sein, insbesondere angesichts der Meldepflichten, die in neuen Gesetzen, etwa der Datenschutz-Grundverordnung, vorgesehen sind, oder zur Einhaltung der Vorschriften von Versicherungen im Zusammenhang mit IT-Sicherheit.

Ein gut definierter und getesteter Reaktionsplan ist bei Vorfällen unerlässlich, um dafür zu sorgen, dass alle Verpflichtungen und Anforderungen erfüllt werden. Eine weitest mögliche Automatisierung dieses Verfahrens trägt erheblich dazu bei, den operativen Aufwand zu reduzieren.

Je länger sich Mitarbeiter mit einem Sicherheitsvorfall beschäftigen müssen, desto höher der Einfluss auf Produktivität und Geschäftsrisiko. Das wichtigste Ziel sollte darin bestehen, weniger Zeit mit der Untersuchung und Abhilfemaßnahmen zu verbringen, idealerweise durch einen Ansatz, mit dem die Reaktion auf derartige Vorfälle standardisiert und automatisiert wird.

Sie haben Mühe, mit der Anzahl der Vorfälle fertig zu werden. Anstatt mehr Mitarbeiter hinzuzuziehen, um die Aufgabe zu bewältigen, sollten Sie Wege finden, die Erkennung und Abhilfemaßnahmen effektiver zu gestalten – z. B. durch Automatisierung und Prioritätensetzung.

Was man nicht messen kann, kann man nicht effektiv sichern. Und Sie führen nicht genug Messungen durch, um das Ausmaß und die Auswirkungen einer Sicherheitsverletzung einschätzen zu können. Ein proaktiver Ansatz bei der Erfassung und Analyse von Informationen hilft Ihnen nicht nur, Sicherheitsvorfälle zuverlässiger und schneller zu entdecken, sondern auch, den Vorfall durch Reverse Engineering nachzuvollziehen, damit Sie Ihre Sicherheitsmaßnahmen und Ihr Risikoprofil verbessern und zukünftigen Angriffen entgegenwirken können.

Wichtige Hilfestellung

Die Sicherheit ist in der Regel eines der größten Hindernisse für neue IT-Initiativen, von der Entwicklung und Implementierung neuer Anwendungen und Services bis hin zur Nutzung neuer IT-Architekturen wie der Hybrid-Cloud. Proaktive Überwachung der IT-Sicherheit, Erkennung von Vorfällen und Reaktion auf Vorfälle – auf einer standardisierten Plattform mit Automatisierung und Analyse – entwickelt sich zu einem der Unterscheidungsmerkmale, mit denen sich die Top-Performer unter den digitalen Unternehmen, die sich schnell mit den Marktbedingungen entwickeln können, vom Rest abheben. Dieses Ziel lässt sich nicht ohne Risiken und Tücken erreichen:

- Zuallererst brauchen Sie einen Plan: Sicherheit muss gut überlegt sein. Versuchen Sie deshalb bewusst, nicht einfach Produkte zu kaufen, wenn Sie Lücken entdecken. Nutzen Sie die Kompetenzen unabhängiger Sicherheitsexperten, die sich ihre Erfahrung und Einblicke mühsam erarbeitet haben. Lassen Sie sich helfen, Lösungen aufzubauen, die sich bewährt haben und leicht zu verwalten sind.
- Allzu viel ist ungesund: Es mag die beste Lösung erscheinen, alles umzuwerfen und von Neuem zu beginnen. Das ist aber selten ein produktiver Ansatz. Stattdessen sollten Sie versuchen, Ihre Kompetenzen in ausgewählten Bereichen zu verbessern, und dann auf diesem Ansatz aufbauen. Mit steigendem Verbreitungsgrad und besserer Erfahrung kann die IT-Infrastruktur erweitert werden, um von den Fortschritten zu profitieren.
- Bleiben Sie flexibel: Wir wissen nicht, was die Zukunft bringt. Wir wissen aber, dass eine Bindung an firmeneigene Schnittstellen die Sicherung von IT-Beständen erschwert, wenn sie sich in Zukunft weiterentwickeln und wandeln. Suchen Sie nach Lösungen, die sich gut als Stack integrieren lassen und die eine Erweiterung durch offene, stabile und gut definierte APIs und Schnittstellen unterstützen.