DELL Technologies

# Die menschliche Seite der Cybersicherheit

## Stellen Sie sich das Worst-Case-Szenario vor.

Ihr gesamtes Rechenzentrum wurde durch einen raffinierten Ransomwareangriff heruntergefahren. Sales, Kundendienst und die Finanzabteilung sind außer Gefecht gesetzt. Sie sind eine leitende IT-Führungskraft, die für die Wiederherstellung der Systeme verantwortlich ist, aber eine Lösung zu finden, hat sich als schwierig erwiesen.

Ihr Team, das ohnehin schon unterbesetzt war, arbeitet seit Wochen fast ohne Pausen oder Urlaub. Einige MitarbeiterInnen haben ***bis zu 36 Stunden durchgehend*** ohne Schlaf gearbeitet. Sie befürchten, dass Müdigkeit zu schlechten Entscheidungen führt und möglicherweise die Recovery selbst gefährdet.

Sie benötigen dringend zusätzliche Ressourcen, die sofort einspringen und helfen können, das Problem zu beheben, aber wo finden Sie sie?

Dieses Szenario mag wie der Anfang eines Romans klingen, basiert aber auf den tatsächlichen Erfahrungen von Kunden von Dell. Es hebt ein erhebliches Problem in der heutigen Cybersicherheitsumgebung hervor: Der menschliche Faktor.

Aktuelle Daten deuten darauf hin, dass in der Branche fast 5 Millionen SicherheitsexpertInnen fehlen. Während der Ressourcenbedarf während eines Vorfalls am stärksten zu spüren ist, müssen die Lösungen bereits viel früher ansetzen.

## Der erste Schritt: Aufbau und Ausbau einer Talentpipeline

Der erste Schritt, um sicherzustellen, dass Sie über die erforderlichen Ressourcen verfügen, besteht darin, eine Talentpipeline aufzubauen:

**Anwerbung von HochschulabsolventInnen und Praktika**

Die Zusammenarbeit mit lokalen Universitäten und technischen Schulen kann einen steten Strom von Nachwuchstalenten gewährleisten. Diese Personen können über die Zeit hinweg zu leistungsstarken Teammitgliedern gefördert werden.

**Fortlaufende Schulungen und Entwicklung**

Während Zeit und Budget ständig unter Druck stehen, müssen CybersicherheitsexpertInnen mit Änderungen bei Tools und Bedrohungen Schritt halten.

**Fokus auf die Mitarbeiterbindung**

Gute Fachkräfte sind sehr gefragt, insbesondere wenn sie Erfahrung im Umgang mit Angriffen haben. Wenn Sie Ihre Spitzenkräfte nicht binden, wird es jemand anderes tun.

Selbst ein starkes Team reicht möglicherweise nicht aus, um den Stress während eines Angriffs zu bewältigen. Planen Sie daher im Voraus und suchen Sie sich zusätzliche Unterstützung, bevor Sie sie brauchen:

**Ressourcen von Drittanbietern prüfen**

Unternehmen, die sich auf Cybersicherheitsberatung und Personalverstärkung spezialisiert haben, können Ihr Team sowohl im laufenden Betrieb als auch bei Incidents unterstützen. Bauen Sie Beziehungen zu diesen Unternehmen auf, auch wenn Sie sie jetzt nicht benötigen, sodass Sie bei Bedarf Zugriff auf diese Ressourcen haben.

Dell bietet eine Reihe von Dienstleistungen an, die bestehende Teams unterstützen können, darunter virtueller CISO (vCISO), Incident Response und Cybersicherheitsberatung.

**Einsatz von KI**

Nutzen Sie die neuen KI-Funktionen, die in Cybersicherheitstools integriert sind, wie z. B. Protokollanalyse, Anomalieerkennung, Triage von niedrigschwelligen Warnmeldungen oder spezielle Schulungen, um Ressourcenlücken zu schließen und betriebliche Anforderungen zu erfüllen, sodass Ihre Teammitglieder sich auf wichtigere Aufgaben konzentrieren können.

## Ressourcenherausforderungen sind während eines Cyberangriffs am größten

Wie das erste Szenario veranschaulicht hat, kann ein großer Cyberangriff Ihr Unternehmen beeinträchtigen und wichtige Systeme und Geschäftsabläufe lahmlegen. Jede Minute kostet das Unternehmen Geld und das Cybersicherheitsteam steht unter enormen Druck, das Problem zu beheben.

Wenn Sie sicherstellen, dass Ihre Teams möglichst auf dem neuesten Stand sind, wirkt sich dies direkt auf die Incident Response und den damit verbundenen Stress für das Team aus.

Denken Sie daran, dass Schulungen über die SicherheitsexpertInnen hinaus auf alle MitarbeiterInnen ausgedehnt werden müssen, da sie die erste Verteidigungslinie sind.

Diese Geschichte unterstreicht eine zentrale Herausforderung: Die Cyberabwehr ist letztlich menschlich. Sie haben Grenzen, und wenn diese Grenzen überschritten werden, können selbst die stärksten Fachleute scheitern. Mentale Ermüdung, Stress und Burnout sind jetzt kritische Faktoren für den Cybersicherheitsstatus.



DELL Technologies

Auch wenn es keine einzige Lösung für diese Herausforderung gibt, können die folgenden Strategien viel bewirken:

**Aufbau einer starken Team- und Talentpipeline**

Die grundlegendste Lösung für dieses Problem besteht darin, es gar nicht erst zu einem Notfall kommen zu lassen – bauen Sie ein starkes Team mit Redundanzen auf.

**Planung für die menschliche Seite eines Angriffs**

Incident-Response-Pläne sind von entscheidender Bedeutung und MÜSSEN Pläne für das Mitarbeitermanagement, die Planung und den Umgang mit Ausfällen von MitarbeiterInnen enthalten.

**Nutzung von Drittanbieter-Ressourcen**

Externe CybersicherheitsberaterInnen können Ihr Team erweitern. Die Incident Response-Services von Dell können beispielsweise innerhalb weniger Stunden ein Expertenteam vor Ort bereitstellen, das sofort mit der Analyse, Eindämmung und Behebung des Problems beginnen kann. Wir haben vielen Kunden geholfen, Cyberangriffe zu überwinden.

## KI kann helfen, ist aber kein Allheilmittel

KI bietet enorme Möglichkeiten zur Verbesserung von Cybersicherheits-Tools und -Programmen. Ihre Möglichkeiten reichen letztendlich von vorausschauenden Analysen über die Entwicklung maßgeschneiderter Schulungsprogramme bis hin zur proaktiven Bekämpfung von Bedrohungen, bevor diese sich ausweiten können.

Vielleicht noch wichtiger ist, dass KI Verteidigern während eines Vorfalls ein Echtzeit-Unterstützungssystem bieten kann. Modelle für maschinelles Lernen, die anhand historischer Angriffsdaten trainiert wurden, können auf der Grundlage ähnlicher Ereignisse in der Vergangenheit Maßnahmen empfehlen.

Mit dem Einzug der natürlichen Sprachverarbeitung in Cybersicherheitstools erhalten Analysten die Möglichkeit, direkt mit ihren Systemen zu interagieren, Bedrohungen zu erkennen und Lösungen umzusetzen.

Künstliche Intelligenz kann auch Verhaltensmuster überwachen, um zu erkennen, wenn ein/e menschliche/r AnalystIn wiederholt Fehler macht – möglicherweise aufgrund von Erschöpfung –, und einen Wechsel der Schicht oder eine neue Perspektive veranlassen.

Während Cybersicherheitstools zunehmend ausgefeiltere KI-Tools integrieren, befinden sich viele der leistungsfähigsten Funktionen noch in der Entwicklung. Beachten Sie, dass KI derzeit noch nicht die Fähigkeiten einer erfahrenen Fachkraft ersetzen kann, ***insbesondere wenn diese bereits Erfahrungen mit Angriffen gesammelt hat.***

## Empfehlungen zur Nutzung von KI:

**Erfahren Sie, wie die Tools Ihren Sicherheitsbetrieb unterstützen können**

Führen Sie eine detaillierte Analyse der KI-Tools durch und implementieren Sie sie dort, wo sie am effektivsten sein können. Mögliche einfach zu bewältigende Aufgaben sind die Erkennung von Advanced Threats, die Automatisierung sich wiederholender Aufgaben und der Einsatz von KI im Identitätsmanagement.

> „Es empfiehlt sich, einen Partner zu haben, der sich um Incident Response, die Behebung von Problemen und die Recovery kümmert.“
>
> ***Jason Rosselot***
> *VP, Cybersecurity und Business Unit Security Officer, Dell Technologies*

**Planen Sie für die Zukunft von KI**

Verstehen Sie, wann neue Funktionen verfügbar werden und wie sie Ihrem Team zugutekommen, und entwickeln Sie einen Plan für deren Implementierung.

**Integration von KI in die Personalplanung**

Da die Automatisierung manuelle Aufgaben reduziert, muss sich die Zusammensetzung Ihres Sicherheitsteams weiterentwickeln. Möglicherweise benötigen Sie Ressourcen auf höherer Ebene, um Sicherheitsinformationen zu analysieren und darauf zu reagieren, anstatt sie zu kompilieren. Passen Sie Ihre Einstellungs- und Entwicklungsstrategien entsprechend an.

Künstliche Intelligenz wird ein bedeutender Teil Ihrer Cybersicherheitsvorgänge werden, wenn sie dies nicht schon ist. Denken Sie jedoch daran, dass es keinen Ersatz für qualifizierte und erfahrene Fachkräfte gibt. Ziel sollte es sein, den Betrieb mithilfe von KI zu automatisieren und das Personal effektiver arbeiten zu lassen, um letztendlich Angriffe zu verhindern und deren Auswirkungen zu minimieren, wenn sie auftreten.

## Förderung einer ausgereifteren Cybersicherheit: Ein Schritt nach dem anderen

Wie alles im Bereich Cybersicherheit ist auch die Berücksichtigung des menschlichen Faktors ein Prozess und kein Ziel an sich. Inkrementelle Maßnahmen und selbst kleine Fortschritte machen einen Unterschied und summieren sich im Laufe der Zeit. Es ist wichtig, daran zu denken, dass selbst die besten Technologie- und Sicherheitstools letztendlich nur so gut sind wie die Menschen, die sie ausführen.



DELL Technologies

## Dell Produkte und Lösungen, die helfen können

| Dell Lösung | Beschreibung |
|---|---|
| Incident Response-Services | Ein Team aus branchenzertifizierten CybersicherheitsexpertInnen steht für eine schnelle Reaktion im Falle eines Cyberangriffs bereit. Wir arbeiten mit Ihnen zusammen, um die Bedrohungen zu beseitigen, bis die normalen Betriebsabläufe wieder aufgenommen wurden. |
| Beratungsservices für Cybersicherheit | Kompetente Beratung, die Ihnen dabei hilft, Schwachstellen in Ihrer Sicherheitsstrategie zu erkennen und zu beheben, Ihre Ressourcen und Daten zu schützen und eine kontinuierliche Überwachung und Governance zu ermöglichen. |
| vCISO | Virtual Chief Information Security Officer, bietet Cybersicherheits-Fachkompetenz und kann bei der Erkennung und Verwaltung von Risiken und der strategischen Entscheidungsfindung helfen. |
| Managed Detection and Response | Reduziert den manuellen Aufwand und optimiert die täglichen Sicherheitsabläufe durch Überwachung, Erkennung von Bedrohungen, Untersuchung und schnelle Reaktion für Endgeräte, Netzwerk und Cloud. Kunden wählen ihre bevorzugte XDR-Plattform (SecureWorks® Taegis™ XDR, CrowdStrike Falcon® XDR oder Microsoft Defender XDR) aus und erhalten fachkundige Beratung, vierteljährliche Berichte und bis zu 40 jährliche Incident-Response-Stunden. |

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **dell.com/cybersecuritymonth**.



DELL Technologies