DELL Technologies

White Paper

DELL MANAGED DETECTION AND RESPONSE

Die umfassende verwaltete Sicherheitslösung für mittelständische und kleinere Unternehmen

ZUSAMMENFASSUNG

Cyberangriffe auf Unternehmen nehmen zu. Das Internet Complaint Center des FBI stellte 2021 eine Steigerung von 69 % gegenüber dem Vorjahr fest und berichtete von Verlusten von insgesamt 4,2 Milliarden US-Dollar.[1] Es sind zwar die Angriffe auf große Unternehmen, die die Schlagzeilen machen, in Wirklichkeit aber sind Unternehmen jeder Größe gefährdet. Kleine Unternehmen, denen die umfangreichen Ressourcen großer Unternehmen fehlen, sind dabei besonders anfällig.

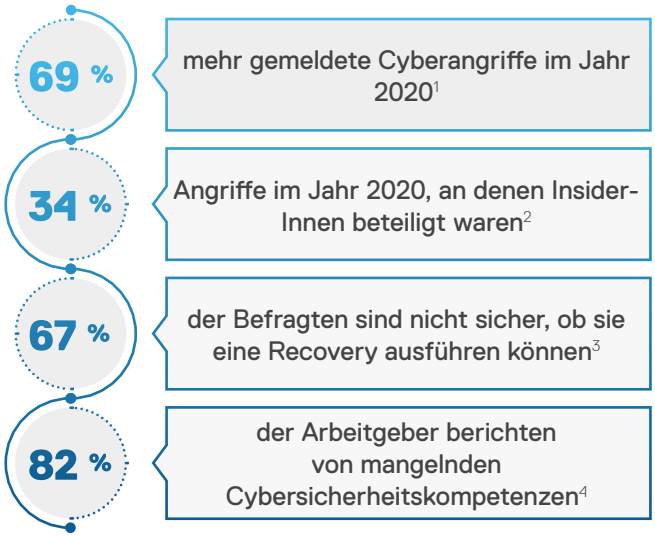
Cybersicherheit spielt beim Schutz von Datenbeständen, Betriebsabläufen und Business Continuity eine kritische Rolle. Große Unternehmen verfügen oft über dedizierte Sicherheitsteams mit den neuesten Technologien, Methoden und Informationen. Mittelständische und kleinere Unternehmen haben jedoch möglicherweise nur eine(n) oder zwei SicherheitsspezialistInnen, die zunehmend komplexe Arrays von Sicherheits-Appliances und Softwaretools managen und betreiben müssen.

Eine zunehmende Herausforderung für die IT

Die Flut von Angriffen auf Endpunkte, Server, Anwendungen, Netzwerke und die Cloud bringt ein immenses Aufkommen an Warnmeldungen mit sich, das die Sicherheits- und IT-Teams schnell überfordert. Außerdem entwickeln die AngreiferInnen ihre Techniken immer weiter und umgehen bisher effektive Verteidigungsmechanismen mit großer Geschicklichkeit. Ein angemessener Schutz der IT-Umgebungen erfordert in den 2020er Jahren ein 24x7x365-Monitoring mit entsprechenden Reaktionen durch dedizierte ExpertInnen.

Wenn die IT-Verantwortlichen mittelständischer und kleinerer Unternehmen ausreichend IT-Personal und Budgetmittel für Cybersicherheit bereitstellen, geht dies zulasten wichtiger Bereiche wie der Anwendungsentwicklung und DevOps. Tatsache ist, dass der Schutz vor den Angriffen von heute eine große Investition in Talente, Tools und Betriebsabläufe erfordert, die sich viele Unternehmen jedoch einfach nicht leisten können.

Cyberangriffe stellen eine größere Bedrohung dar als je zuvor



Die Lösung: Managed Detection and Response

Folglich ziehen immer mehr Unternehmen MDR-Lösungen (Managed Detection and Response) von externen Serviceanbietern in Betracht. Aber wie können IT-Entscheidungstragende einen erstklassigen MDR-Partner erkennen?

Ein geeigneter MDR-Lösungsanbieter muss eine Technologie implementieren, die bekannte Arten von Bedrohungen erkennt, falsch positive Ergebnisse minimiert, Ereignisse korreliert, die Aktivitätssequenz von Eindringlingen verfolgt und Eindämmungs- und Präventionsmaßnahmen automatisiert. Ein solcher Anbieter benötigt ein Team aus hochqualifizierten und erfahrenen SicherheitsexpertInnen, um Warnmeldungen 24x7x365 zu analysieren, Bedrohungen abzuwehren und nach neuen Bedrohungstypen Ausschau zu halten.

Die Bereitstellung von MDR-Services erfordert den Aufbau von Sicherheitsabläufen sowie die Einrichtung und Optimierung zugehöriger Prozesse. Darüber hinaus benötigen AnalystInnen Tools für den Wissensaustausch sowie regelmäßige Schulungen, um über die neuesten Bedrohungen und Techniken auf dem Laufenden zu bleiben.

Obwohl viele Serviceanbieter Managed Services für die Erkennung und Reaktion anbieten, verfügen nur wenige über die Kapazitäten und Fähigkeiten, die für wirkliche Spitzenleistung erforderlich sind.

Dell Managed Detection and Response ist eine vollständig verwaltete, durchgängige 24x7-Lösung, die Bedrohungen in der gesamten IT-Umgebung eines Unternehmens überwacht, erkennt, untersucht und abwehrt. Egal ob ein Unternehmen 50 oder mehrere Tausend Endpunkte hat – Dell MDR verbessert schnell und deutlich den Sicherheitsstatus des Unternehmens und verringert zugleich die Belastung für das IT-Personal. Dell MDR profitiert von der Fähigkeit von Dell, in Belegschaft, Prozesse und Tools zu investieren, um mittelständischen und kleineren Unternehmen eine Lösung für das Monitoring von Cybersicherheit mit entsprechenden Gegenmaßnahmen der Enterprise-Klasse bereitzustellen.

Die wichtigsten Gründe, warum Unternehmen MDR-Lösungen (Managed Detection and Response) nutzen

- **Zugang zu ansonsten schwer zu findenden CybersicherheitsexpertInnen**
- **Umfassende Funktionen für Monitoring, Erkennung und Reaktion**
- **Geringere Belastung für IT-Personal, das sich nun auf DevOps konzentrieren kann**

DIE BEDROHUNGSLANDSCHAFT VON HEUTE

Die AngreiferInnen von heute gehen methodisch vor und überlegen sich wochen- oder auch monatelang, wie sie sich Zugriff auf wertvolle Anwendungen und Daten verschaffen können. Nachdem sie eine Gelegenheit erkannt haben, können sie das Öffnen von E-Mails ausnutzen oder Phishing-E-Mails senden, um NutzerInnen dazu zu bringen, einen schädlichen Anhang zu öffnen. Die Erkennung und Reaktion sind wesentliche Elemente eines umfassenden Cybersicherheitsprogramms, ebenso wie Mitarbeiterschulungen, Cybersicherheitsbewertungen, Schwachstellen- und Durchdringungstests, Ausfallsicherheit, Recovery-Planung usw.

Nachdem sich die AngreiferInnen Zugriff verschafft haben, möchten sie sich zuerst eine Ausgangsbasis errichten, von der aus sie den Umfang des Angriffs erweitern können. Auch hier nehmen sie sich Zeit, ihre Position in der Infrastruktur des Unternehmens zu festigen. So zielen Ransomware-Angriffe nicht nur auf Geschäftssysteme ab, sondern sind oft auch darauf ausgerichtet, die Backupsysteme eines Unternehmens offline zu schalten und den Zugriff auf die Backups zu blockieren. Dies kann dazu führen, dass ein Unternehmen keine Wiederherstellungen mehr durchführen kann, sodass die Zahlung des Lösegelds die einzige Möglichkeit ist, den Betrieb wiederaufzunehmen.

Ausgefeilte und ständig aktualisierte Erkennungs- und Reaktionsfunktionen sind unverzichtbar, um Angriffe und andere Signale zu erkennen. Eine frühzeitige Warnung gibt dem Unternehmen die Möglichkeit, den Schaden, der sich durch den Angriff ergeben könnte, zu minimieren – bevor er sich weiter ausbreitet.

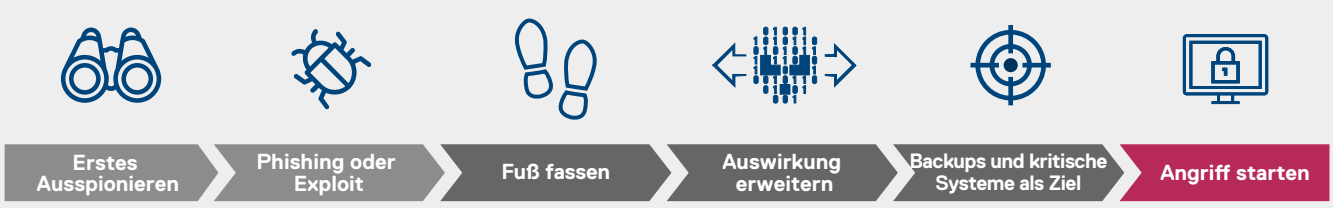
Die Unternehmen haben eine Vielzahl an Cybersicherheitstools implementiert, z. B. für Passwortauditing, Netzwerktests, Schwachstellenscans, Verschlüsselung, Monitoring und Bedrohungserkennung, von denen Warnmeldungen an die IT gesendet werden. Allein die Menge dieser Meldungen ist eine Herausforderung, die jedoch umso größer ist, wenn man berücksichtigt, wie schwierig es ist, Ereignisse toolübergreifend zu korrelieren. Darüber hinaus kostet die Aufrechterhaltung der Kenntnisse all dieser Technologien dem IT-Sicherheitspersonal enorm viel Zeit.

MDR erfordert ein Team aus Fachleuten mit jahrelanger Cybersicherheitserfahrung und Kenntnissen in den Bereichen Systemadministration, Cyberforensik, Bedrohungsuntersuchung und Penetrationstests. Solche Fachkräfte sind nicht nur schwer zu finden, sondern auch teuer. Außerdem werden sie oft von attraktiveren, ausgabenstärkeren Unternehmen wegrekrutiert. Die Umfrage „State of the CIO“ aus dem Jahr 2021 ergab, dass Fachkräfte im Bereich Cybersicherheit in der IT als am schwierigsten zu besetzen sind.[5] Die Bindung vorhandener SicherheitsanalystInnen sowie die Neubesetzung all jener Kräfte, die das Unternehmen verlassen, ist für die IT-Verantwortlichen ein schier endloser Kampf.

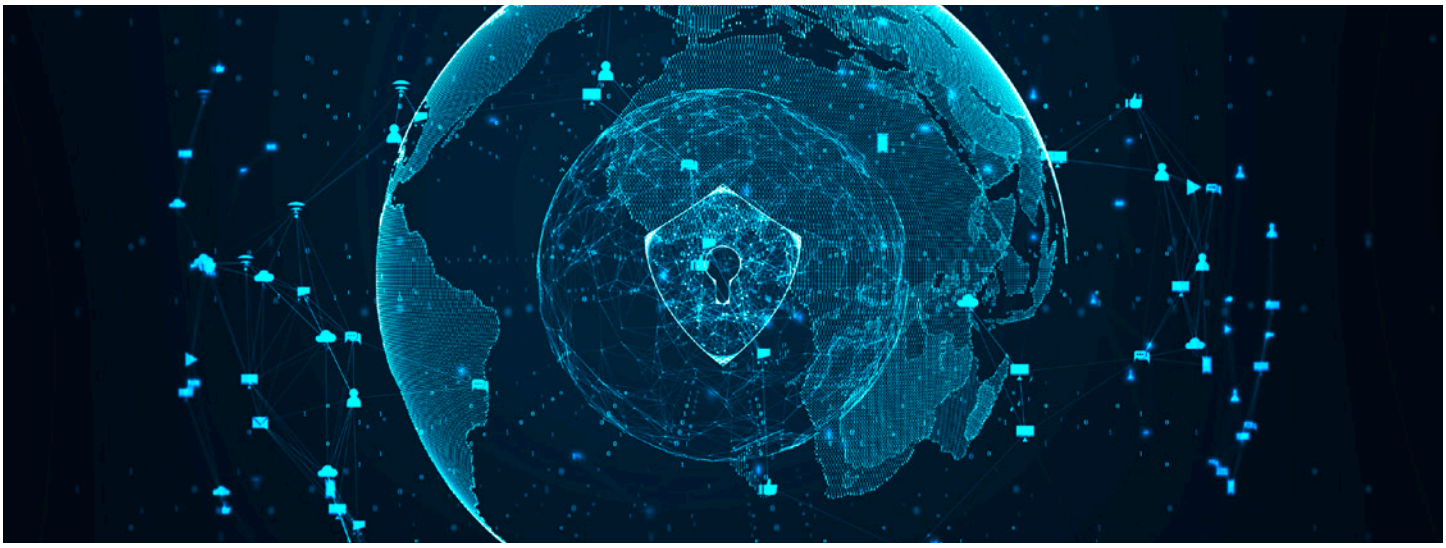
Aber auch nach dem Erwerb der grundlegenden Tools und Talente müssen die Unternehmen 24x7-Sicherheitsabläufe und -einrichtungen aufbauen.

Abbildung 1: Strategie der AngreiferInnen

Die Verweildauer beträgt im Durchschnitt mehr als 100 Tage, bevor der eigentliche Angriff beginnt.



Monitoring und Erkennung sind entscheidend, um Angriffe von vornherein zu verhindern.



Mit Dell Managed Detection and Response Services sind erstklassige Funktionen in Reichweite

Es ist kein Wunder, dass mittelständische und kleinere Unternehmen oft Schwierigkeiten haben, sich angemessen zu verteidigen. Die Cybersicherheitslandschaft hat sich zu einem Kaleidoskop von Bedrohungen entwickelt, das sich ständig wandelt. Das große Ausmaß an Angriffsaktivitäten hat den Personalbedarf steigern lassen, aber auch die Komplexität der Angriffe hat die Anforderungen an die MitarbeiterInnen erhöht.

Dell Managed Detection and Response erweitert Ihr Sicherheitsteam um CybersicherheitsexpertInnen, Tools und Betriebsfunktionen, die mit denen der größten globalen Unternehmen vergleichbar sind. Dell MDR reduziert die Belastung für Ihr IT-Team, mindert die Risiken und verbessert den Sicherheitsstatus Ihres Unternehmens erheblich – sodass Sie sich auf Ihre geschäftlichen Prioritäten konzentrieren können.

Dell Managed Detection and Response ist eine vollständig integrierte Kombination aus Technologie, Fachwissen und Betriebsabläufen. Der Service stützt sich auf das Wissen der SicherheitsanalystInnen von Dell Technologies, die Unternehmen auf der ganzen Welt jahrelang dabei geholfen haben, ihren Betrieb besser zu schützen. Dell MDR macht sich außerdem die Leistungsfähigkeit von Secureworks® Taegis™ XDR zunutze. Dies ist eine fortschrittliche Softwareplattform für Sicherheitsanalysen, die mehr als 20 Jahre bewährtes Know-how, Threat Intelligence aus der Praxis und Forschung sowie Fachwissen bei der Erkennung und Reaktion auf raffinierte Bedrohungen vereint.

Secureworks Taegis XDR

Secureworks Taegis XDR ist eine speziell entwickelte Cybersicherheitsplattform, die Sicherheitsbedenken mit einer Big-Data-basierten Lösung ausräumt. Taegis XDR ist eine Cloud-native Plattform und umfasst kontinuierliche Bewertungen von Telemetriedaten und Ereignissen verschiedener Angriffsvektoren, gestützt auf maschinellem Lernen und Deep Learning und angereichert mit umfassenden Bedrohungsdaten.

Gründe für Dell Managed Detection and Response

Personal

- **Erfahrene CybersicherheitsexpertInnen**
- **Für Taegis XDR zertifizierte AnalystInnen**
- **Zertifizierungen, einschließlich CEH, GIAC SANS, CISSP und CompTIA**

Technologie

- **Branchenführende Secureworks Taegis XDR-Plattform für die Sicherheitsanalyse**
- **Kontinuierliches, durchgängiges Bedrohungsmonitoring unter Verwendung von Telemetriedaten von unterschiedlichsten Endpunkten, Netzwerken und Clouds**

Prozess

- **Kurze Problemlösungszeit**
- **24x7x365-Bereitschaft**
- **Unterstützung beim Agent-Rollout**
- **40 Stunden Unterstützung pro Quartal bei Remotekorrektur**
- **40 Stunden pro Jahr für Initiierung der Reaktion auf Incidents**

Zuverlässiger Partner

- **Genießt weltweites Vertrauen für Geräte- und Infrastruktursupport**
- **Mehr als 20 Jahre Innovationen bei Ausfallsicherheit für Unternehmen**
- **Kontinuierliche Investitionen in Belegschaft, Prozesse, Tools**

Abbildung 2: Threat Intelligence

Die einzige Möglichkeit, raffinierte Angriffe zu erkennen und darauf zu reagieren, besteht darin, zuallererst zu verstehen, wie die AngreiferInnen vorgehen und was ihre Motivation ist. Jedes Jahr wickelt das Secureworks-Team hinter XDR ca. 1.000 Incident-Response-Projekte ab. Dies verschafft den ExpertInnen einen deutlichen Vorteil, wenn es darum geht, festzustellen, wie sich Strategien, Techniken und Prozesse der AngreiferInnen, die erfolgreich in Unternehmen eindringen, kontinuierlich ändern.

Taegis XDR analysiert für die Bedrohungserkennung sicherheitsrelevante Daten, die von Endpunkten, Netzwerken, Cloud-Systemen und lokalen Geschäftssystemen erfasst werden. XDR ist eine komplett offene Plattform, die die vorhandene Sicherheitsinfrastruktur ergänzt, um alle Anforderungen abzudecken und bereits getätigte Investitionen zu schützen.

XDR bietet automatisierte Reaktionen, Korrekturen und Einblicke, um die Effizienz von Sicherheitsmaßnahmen zu erhöhen und den Reaktionsteams die nötige Transparenz zu bieten, damit sie bei Auftreten einer Bedrohung aktiv werden können. Kunden von Dell MDR profitieren von der Threat Intelligence, die mit Hunderttausenden von Datenpunkten entwickelt und kundenübergreifend kompiliert wurde, sowie von gemeinsamen Intelligence Services weltweit.

Die besten SicherheitsexpertInnen arbeiten für Sie

Ein globales Team hochqualifizierter SicherheitsanalystInnen ist unaufhörlich auf der Suche nach Problemen in Ihren Systemen. Die kompetenten CybersicherheitsexpertInnen von Dell haben Erfahrung in allen Phasen der Bedrohungserkennung und -entschärfung, einschließlich Erkennung und Untersuchung von Bedrohungen, Endpunktsicherheit sowie Reaktion auf und Recovery von Incidents. Die AnalystInnen von Dell sind XDR-zertifiziert und verfügen über eine Reihe anderer behördlicher und branchenweit anerkannter Zertifizierungen, darunter z. B. CEH, GIAC SANS, CISSP und CompTIA. Das verteilte Security Operation Center von Dell MDR ist 24x7x365 verfügbar.

Das Dell MDR-Team macht sich mit Betrieb und IT-Infrastruktur eines Unternehmens vertraut. Es nutzt maschinelles Lernen und kuratierte Bedrohungsinformationen aus Tausenden von IT-Umgebungen, die über XDR bereitgestellt werden, um Ihre Umgebung zu überwachen. Das Dell MDR-Team tritt sofort in Aktion, wenn eine Warnung angezeigt wird, und untersucht dann die Warnungsdaten, um Verbindungen und Muster zu identifizieren, die nur geschulte und erfahrene SicherheitsanalystInnen erkennen würden. Anschließend empfiehlt das Team den Mitgliedern des Reaktionsteams des Unternehmens die beste Vorgehensweise.

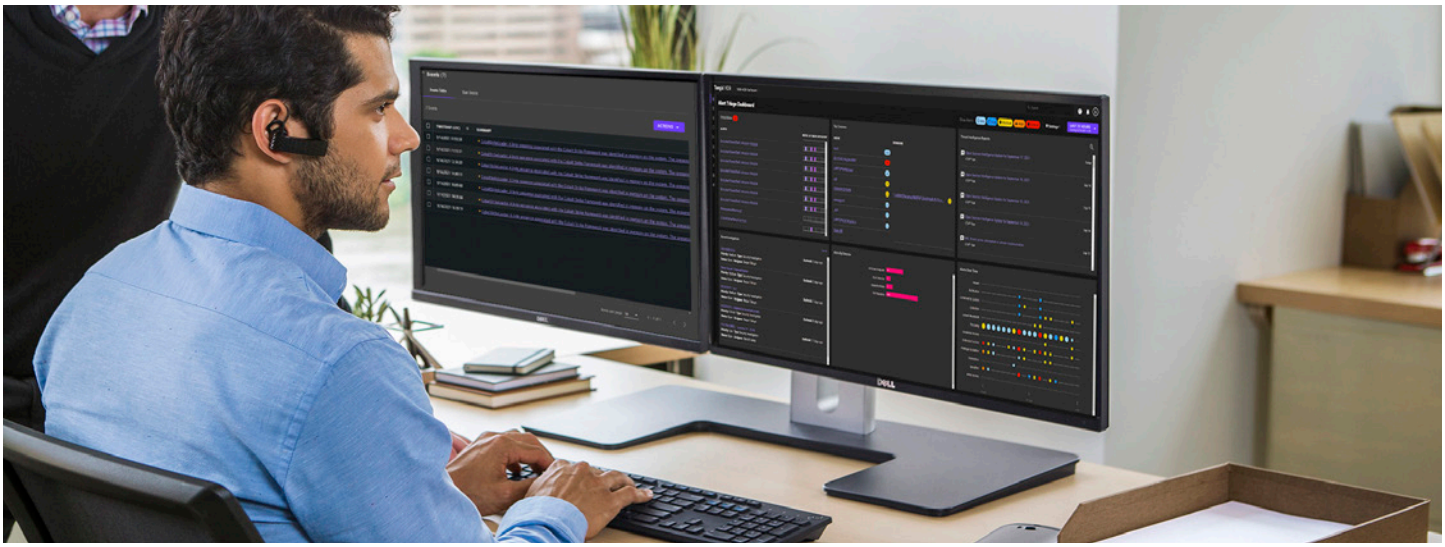
Dell MDR ist Teil der jahrzehntelangen Bemühungen von Dell, eine IT-Serviceorganisation von Weltklasse aufzubauen. Das bedeutet, dass die Dell MDR-CybersicherheitsexpertInnen nicht nur hervorragende Unterstützung bei der Abwehr von Bedrohungen leisten, sondern auch über die Fähigkeiten und das Know-how verfügen, um sie für jedes Unternehmen zu managen.

Bedrohungssuche – Identifizieren von Bedrohungen, die automatisierte Systeme umgehen können

AngreiferInnen sind die automatisierten Erkennungssysteme natürlich bekannt, weshalb sie daran arbeiten, neue Angriffsarten oder Variationen vorhandener Angriffsarten zu entwickeln, um diese Systeme zu umgehen. Bei einem System wie Taegis XDR ist das zwar nicht einfach, aber möglich.

SicherheitsanalystInnen nutzen die Bedrohungssuche, um solche „heimlichen“ Bedrohungen zu erkennen. Im Rahmen der Bedrohungssuche wird nach Anzeichen für eine Kompromittierung gesucht, z. B. mehrere erfolglose Anmeldungen bei einem Konto gefolgt von einer erfolgreichen Anmeldung, ungewöhnliche Anmeldeversuche etwa außerhalb der regulären Geschäftszeiten oder wiederholte Änderungen an einer Datei innerhalb eines kurzen Zeitraums.

An einer effektiven Bedrohungssuche sind sowohl Technologie als auch Menschen beteiligt. Die Taegis XDR-Plattform bietet enorm viele Details zu den Aktivitäten eines Eindringlings. Die Dell MDR-AnalystInnen durchforsten diese Details, um selbst gut verborgene Aktivitäten zu erkennen.



INFORMATIONEN ZU DELL MDR

Nachrichtenmedien berichten von den Schwierigkeiten von Regierungen und globalen Konzernen, Cybersicherheitsbedrohungen einzudämmen. Auch mittelständische und kleinere Unternehmen müssen sich dieser Herausforderung nun nicht mehr allein stellen. Mit Dell MDR hat Ihr Unternehmen Zugang zu hochqualifizierten SicherheitsexpertInnen, die Sie schützen, sowie zur branchenführenden Sicherheitsplattform Secureworks Taegis XDR. Dabei profitiert Ihr Unternehmen von der Fähigkeit von Dell, in Belegschaft, Prozesse und Tools zu investieren, um einen Managed Security Service bereitzustellen, der auf die Anforderungen Ihres Unternehmens zugeschnitten ist. Der Managed Detection and Response Service von Dell bietet Weltklasse-Cybersicherheit, die für alle zugänglich ist.

Weitere Informationen zu Dell MDR

Kontaktieren Sie ein Mitglied unseres MDR-Expertenteams.

1. 69 % mehr Angriffe laut FBI: https://blog.isc2.org/isc2_blog/2021/03/fbi-cybercrime-shot-up-in-2020-amidst-pandemic.html
2. 34 % InsiderInnen: https://www.verizon.com/business/resources/reports/dbir/
3. 67 % sind sich nicht sicher, ob sie ihren Betrieb nach einem verheerenden Cyberangriff wiederherstellen können: www.delltechnologies.com/gdpi
4. 82 % der Arbeitgeber berichten von mangelnden Cybersicherheitskompetenzen: https://www.csis.org/analysis/cybersecurity-workforce-gap
5. 13 am schwierigsten zu besetzende IT-Jobs: https://www.cio.com/article/221772/10-most-difficult-it-jobs-for-employers-to-fill.html

DELL Technologies