MSPs: UMFASSENDER Schutz vor Cyberbedrohungen

WatchGuard®

Inhalt

MSPs:

Ihr letzter Stop in der Abwehr von Cyberbedrohungen

In der schnelllebigen Welt des Eishockeys bedeutet eine konstante Abfolge unerbittlicher Angriffe, dass eine starke Verteidigungsstrategie ausschlaggebend ist. Hockey-Teams sind bei aggressiven Angriffen oft zahlenmäßig unterlegen, müssen aber trotzdem tun, was sie können, um den Gegner davon abzuhalten, Tore zu erzielen.

Gleiches gilt für Cybersicherheit. Unternehmen aller Arten und Größen stehen ausgefeilten Bedrohungsakteuren und Angriffstechniken gegenüber und benötigen eine starke Verteidigung, die in der Lage ist, Gefahren abzuwehren. Und wie im Hockey und vielen anderen Sportarten auch hängt der Erfolg in der Cybersicherheit von einer soliden Strategie und Teamarbeit ab.

Mit einem zuverlässigen Managed Service Provider (MSP) als Kern Ihrer Cybersicherheitsstrategie, der als letzter Stop in der Abwehr fungiert, kann Ihr Team Cyberkriminellen das Handwerk legen.

Fühlen Sie sich überfordert?

Es ist alles andere als einfach, ein modernes Unternehmen in der heutigen Bedrohungslandschaft zu schützen. Die meisten IT- und Sicherheitsteams fühlen sich gegenüber ausgeklügelten Angriffen nur unzureichend gewappnet. Wenn Ihnen diese Herausforderungen bekannt vorkommen, sind Sie nicht allein.

- Unzureichendes Budget für notwendige Sicherheitslösungen und Personal
- Zu wenig Zeit und Bandbreite für wichtige Sicherheitsaufgaben
- Schwierigkeiten bei der Anwerbung und Bindung von Cybersicherheitsexperten aufgrund der anhaltenden Qualifikationslücke
- Komplexe, hybride Belegschaften und IT-Umgebungen
- Die steigende Menge ausgefeilter Sicherheitsbedrohungen
- Die erheblichen Kosten, die durch Ausfallzeiten und Datensicherheitsverletzungen verursacht werden
- Zunehmend strenge, regulatorische Anforderungen
- Ständige Weiterentwicklung und Erweiterung der Technologieoptionen

Wussten Sie schon ...

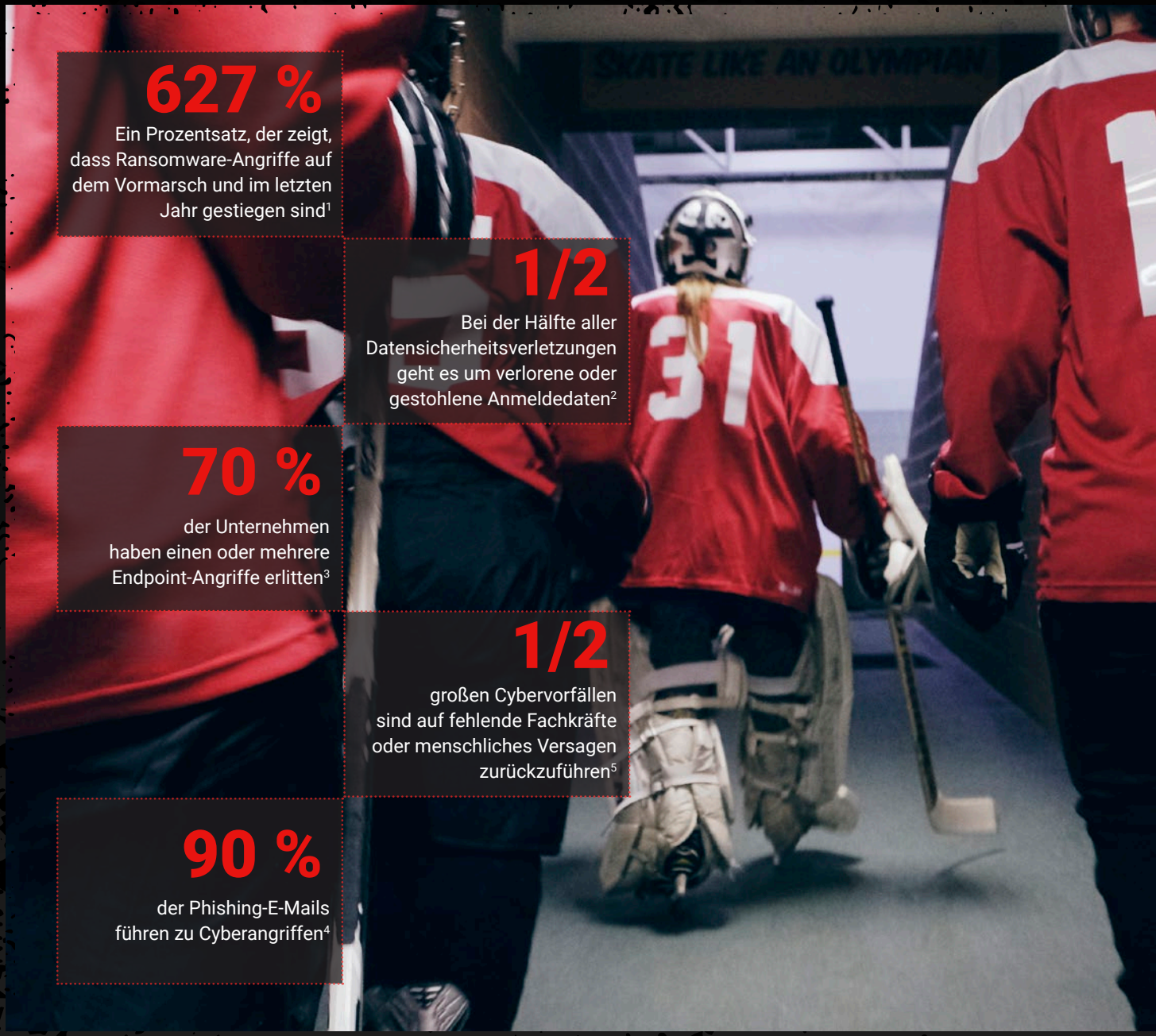
Ein „Penalty Kill“ im Eishockey liegt vor, wenn ein Team in der Unterzahl ist, weil einer oder mehrere seiner Spieler Zeit auf der Strafbank verbringen. Das zahlenmäßig unterlegene Team ist erheblich benachteiligt und muss sich auf defensive Strategien konzentrieren, um Tore zu verhindern. Cybersicherheit kann sich manchmal wie ein endloser Penalty Kill anfühlen.

Womit Sie es zu tun haben: Cyberbedrohungen in Zahlen

Jeden Tag stehen Sie vor einer wachsenden und immer komplexer werdenden Bedrohungslage. Die Wahrscheinlichkeit ist hoch, dass Ihre Teams oft „zahlenmäßig unterlegen" sind, wenn sie versuchen, übergroße Cybergegner abzuwehren, die immer raffinierter und rücksichtsloser vorgehen.

- Ransomware-Angriffe nehmen zu und sind im letzten Jahr um 627 % gestiegen[1]
- Bei der Hälfte aller Datensicherheitsverletzungen geht es um verlorene oder gestohlene Anmeldedaten[2]
- Fast 70 % der Unternehmen haben einen oder mehrere Endpoint-Angriffe erlitten[3]
- 90 % der Cyberangriffe sind auf Phishing-E-Mails zurückzuführen[4]
- Über die Hälfte der großen Cybervorfälle sind auf fehlende Fachkräfte oder menschliches Versagen zurückzuführen[5]

Die Wahrheit ist, dass Sie, um sich gegen Cyberkriminelle durchzusetzen, eine Strategie benötigen, die alle Ihre Schwachstellen abdeckt, Teamarbeit über Ihren gesamten Sicherheits-Stack hinweg sicherstellt und vereinfachte, skalierbare Abläufe ermöglicht.



Quelle: 1. WatchGuard | 2. Verizon | 3. Ponemon | 4.CISA | 5.Gartner

Eine Strategie für eine stärkere Verteidigung

Wie sieht eine erfolgreiche Verteidigungsstrategie aus? Es gibt fünf Schlüsselelemente, die für eine Sicherheitsstrategie wichtig sind, um sich heutzutage vor wachsenden Bedrohungen zu schützen.

1. **Umfassende Sicherheit** – eng integrierte Sicherheitslösungen, die Ihre IT-Umgebungen, Geräte und Anwender (Netzwerk-, Endpoint- und Identitätssicherheitsprodukte und -dienste) schützen können.

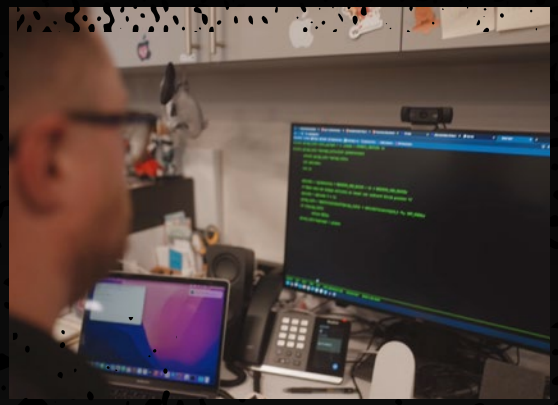
2. **Transparenz und Kontrolle** – eine zentralisierte Sicherheitsmanagementlösung, die Bereitstellungs-, Administrations-, Verwaltungs- und Reportingaufgaben vereint.

3. **Kollektive Intelligenz** – die Möglichkeit, Sicherheitsdaten und Warnungen über Domänen und Sicherheitslösungen hinweg zur Korrelation, Priorisierung und für automatisierte oder manuelle Abhilfemaßnahmen zu teilen, zu erfassen und zu visualisieren.

4. **Operative Ausrichtung** – ein robustes Ökosystem aus Integrationen, APIs und flexiblen Zahlungsoptionen, um Geschäftsanforderungen und skalierbare Sicherheitsvorgänge zu unterstützen.

5. **Automatisierung** – ausgefeilte Automatisierungsfunktionen, die die Sicherheitseffizienz verbessern und Verwaltungsaufgaben optimieren.

Angesichts des Ausmaßes und der Schwere der heutigen Bedrohungen reicht es oftmals nicht aus, sich ausschließlich auf interne Ressourcen und Fachwissen zu verlassen, um diese kritischen Sicherheitselemente zu beschaffen, bereitzustellen und zu verwalten. Die gute Nachricht ist, dass es noch nicht zu spät ist, externe Unterstützung in Betracht zu ziehen, um den Schutz zu erhöhen.



MSPs:
Ihr Cybersicherheits-MVP

Managed Service Provider (MSPs) bieten eine Reihe von Sicherheitsprodukten und -diensten an, die Unternehmen vor Cyberangriffen schützen. Da Cyberangriffe weiterhin zu kostspieligen Sicherheitsverletzungen führen, wenden sich viele Unternehmen an MSPs. Diese fungieren als vertrauenswürdige Berater und haben die erforderliche Zeit und das entsprechende Fachwissen, um Bedrohungen effektiv zu bekämpfen.

- Überbrückung der fehlenden Sicherheitskompetenz durch eine große Anzahl von Cyberexperten
- Laufende Überwachung, Erkennung und Behebung von Bedrohungen
- Bereitstellung eines kosteneffizienten Weges zu einem stärkeren Schutz
- Vereinheitlichung und Vereinfachung verschiedenster Sicherheits-Toolsets
- Entlastung von Mitarbeitern, um sich auf die Kerngeschäfte zu konzentrieren

Viele Unternehmen arbeiten mit MSPs zusammen, um die Sicherheit zu erhöhen.

74 %

Prozentsatz der globalen **IT-Ausgaben**, die über den Channel laufen[1]

91 %

Prozentsatz der globalen **Cybersecurityausgaben**, die über den Channel laufen[2]

93 %

aller Unternehmen nutzen die Möglichkeit, alle oder einen Teil ihrer **Cybersicherheitsaufgaben an MSP/MSSPs auszulagern**[3]

Wussten Sie schon ...

Durch die Entscheidung, mit einem MSP zusammen zu arbeiten, können wichtige Sicherheitsansätze genutzt werden, die sonst außer Reichweite wären. Zum Beispiel verwenden viele MSPs den KI-fähigen Zero-Trust Application Service von WatchGuard, um mit dem Deny-by-Default-Ansatz Endpoint-Sicherheit im großen Maßstab zu gewährleisten. So wird sicherstellt, dass nur sichere Anwendungen und Prozesse auf Ihren Geräten ausgeführt werden.

Quelle: 1. Canalys | 2. Canalys | 3. Pulse

Zusammenarbeit mit einem MSP, der Ihre Sicherheit verwaltet

Jeder MSP ist anders, von den Anbietern, die er verwendet, über die Art und Weise, wie er mit Kunden interagiert, welche Managed Services er anbietet, und so weiter. In ähnlicher Weise hat jedes Unternehmen einzigartige Sicherheits-, Geschäfts- und Betriebsanforderungen. Ergänzen Sie Ihr Team durch den richtigen MSP, und Sie können sich darauf verlassen, dass Sie Bedrohungen umfassend und effektiv abwehren können, um Ihr Unternehmen zu schützen.

Wussten Sie schon ...

Die Nutzung von MDR (Managed Detection and Response) nimmt rasant zu, da Unternehmen nach Möglichkeiten suchen, ihren Schutz zu erhöhen und gleichzeitig die versicherungstechnischen und regulatorischen Vorgaben zu erfüllen. Viele bevorzugen MDR von einem vertrauenswürdigen Service Provider, um die Kosten und Komplexität des Aufbaus und der Verwaltung eines internen Sicherheitsbetriebszentrums zu vermeiden.

Nutzen Sie diese Checkliste, um Ihre Anforderungen darzustellen und zu organisieren, damit Sie diese bei der Prüfung möglicher MSP-Partner als Leitfaden nutzen können, um sicherzustellen, dass sie den Grad an Sicherheit bieten, den Ihr Unternehmen benötigt.

Geschäftszeiten	
☐	Geschäftszeiten (8x5), verlängerte Servicezeiten
☐	Verlängerte Servicezeiten (12-24x5 oder 12-24x7)
☐	Ständige Erreichbarkeit (24x7x365)
Beziehung zum Kunden	
☐	Lösungsexperte für Beschaffungen, Kunden bleiben Eigentümer/Betreiber von Sicherheitslösungen
☐	Beratender Sicherheitsexperte; Mitverantwortung für Sicherheitsdienste
☐	Besitzt und betreibt Sicherheitslösungen im Namen der Kunden; gemessen an SLA/SLO
Transaktionsmodell	
☐	Herkömmliche, projektbasierte Abrechnung
☐	Individuelle Angebote mit einer Mischung aus projektbasierten Rechnungen und Vereinbarungen für Managed Security Services
☐	Serviceverträge mit monatlichen oder jährlichen Zahlungen, inklusive Hardware und/oder Software
Art des Unternehmens	
☐	Große, traditionelle Unternehmen mit zahlreichen Vertriebs- und Kundendienstmitarbeitern und einer kleinen Dienstleistungsproduktlinie mit Administratoren
☐	Große Serviceunternehmen mit Sicherheitsanalysten und weniger traditioneller Struktur
☐	Vollständig dienstleistungsbasiert, mit gestaffelten Sicherheitsanalysten, Threat Huntern, Kundendienstmitarbeitern usw.
Produktverpackung	
☐	Produktbasierte Sets mit umfangreichen Anpassungsmöglichkeiten durch den Kunden und einigen Managed Services-Optionen
☐	Standardpakete mit einigen Zusatz- und Anpassungsoptionen; bereit, einige spezifische Einzelprodukte zusätzlich zu Serviceverträgen zu verkaufen
☐	Standardisierte Managed Security-Paktete mit wenigen Zusatz- oder Anpassungsoptionen
Methode der Servicebereitstellung	
☐	Produktverkauf durch Anbieter oder Vertrieb begrenzter Managed Services; Bereitstellung grundlegender Services zur Sicherheitsüberwachung durch Administratoren, die Warnungen/Protokolle überprüfen
☐	In erster Linie Managed Services-Pakete; bietet einige SOC-Funktionen über ausgelagerte SOC- oder Vendor-Managed Services
☐	Exklusive Managed Services-Pakete; bereitgestellt über ein internes SOC mit einem hoch standardisierten Tech-Stack für erweiterte Sicherheitsangebote

Sie suchen nach umfassendem Schutz vor Cyberbedrohungen?

Die heutigen Bedrohungsakteure gehören zu den härtesten Gegnern überhaupt. Es kann eine große Herausforderung sein, sich ihnen allein entgegenzustellen. Doch das müssen Sie zum Glück gar nicht. Zuerst einmal müssen Sie einen vertrauenswürdigen Partner und Berater finden, der Ihnen hilft, Ihr Unternehmen zu schützen. Überlegen Sie, was Ihre größten Sicherheitsherausforderungen und -anforderungen sind und beginnen Sie, nach Partnern zu suchen, die Ihren Anforderungen entsprechen. Wenn Sie Fragen haben oder Hilfe bei der Suche benötigen, können Sie sich gerne jederzeit an uns wenden! Wir arbeiten mit Unternehmen wie Ihrem zusammen, um Umgebungen, Anwender und Geräte zu schützen.

gid GmbH

040 535 76 - 0

info@gid-gmbh.de

Unsere Produkte nutzen WatchGuard-Technologie. WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Netzwerksicherheit und Intelligence, fortschrittlicher Endpoint-Schutz, Identitätssicherung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1 206 613 0895 WEB www.watchguard.com