Verstehen lernen, wie Fertigungsunternehmen mit Bedrohungslagen umgehen

ein CXO-Prioritätenbericht in Zusammenarbeit mit Quest

Quest

priorities

A Lynchpin Media BRAND

INHALT

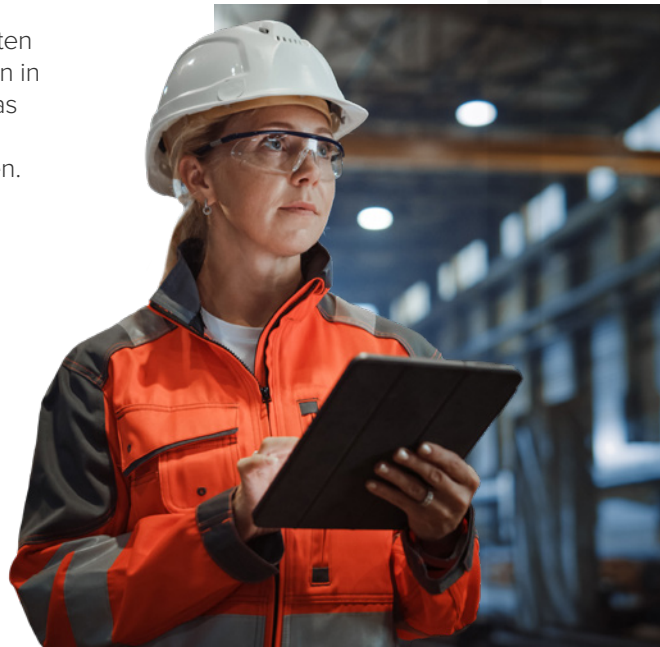
EINLEITUNG

Die sich rasant vergrößernden Angriffsflächen und die sich damit stets weiterentwickelnde Bedrohungslage bringen die fast dreifache Wahrscheinlichkeit mit sich, dass jedes Fertigungsunternehmen Opfer eines Cybersicherheitsereignis werden kann, das groß genug ist, um seinen Produktionsprozess zu stören. DUnd auch die Pandemie spielte bereits eine entscheidende Rolle bei der Aufdeckung von Angriffslagen und nur begrenzten Cybersicherheitstools, was wiederum die Disaster-Recovery-Richtlinien in der Fertigungsindustrie stark ins Rampenlicht gerückt hat.

Als wachsende Bedrohung für die Fertigungsindustrie werden Cyberangriffe zudem immer umfangreicher und ausgefeilter. Wir erleben immer mehr disruptive Angriffe, die sich auf industrielle Prozesse und Unterbrechungen der Lieferkette auswirken. Mit darunter Ransomware sowie Eindringlingeeinen , die Informationsdiebstahl ermöglichen sowie neue Aktivitäten von industriellen Steuerungssystemen, die genau auf Angreifer abzielen.

Die Auswirkungen dieser Fortschritte und des Fehlens von inhärenten Sicherheitskontrollen, die zum Selbstschutz erforderlich sind, führen zu Produktionsausfällen, finanziellen Verlusten in Millionenhöhe, Unterbrechungen der Lieferkette und Reputationsschäden für Unternehmen.

Das verarbeitende Gewerbe zählt außerdem zu den fünf Branchen mit den meisten Cyberangriffen. Daher schlagen Experten vor, dass jedes Fertigungsunternehmen in ganzheitliche Cyber-Management-Programme investieren sollte, die sich über das gesamte Unternehmen erstrecken, um Cyberangriffe zu erkennen, sich davor zu schützen, darauf zu reagieren und sich davon auch letztendlich wieder zu erholen.



Quest

CXO priorities

A Lynchpin Media BRAND

UMFRAGENÜBERSICHT:

Und um noch mehr über diese Thematik zu erfahren, haben wir C-Level-Führungskräfte zu ihren Herausforderungen im Bereich der Cybersicherheit in Großbritannien, Deutschland und Frankreich des gesamten Fertigungssektors befragt. Dieser Bericht untersuchte außerdem die Herausforderungen, mit denen Fertigungsunternehmen bei der Stärkung ihrer Sicherheits- und Disaster-Recovery-Richtlinien konfrontiert sind.

Mit dieser Umfrage wollten wir Folgendes herausfinden:

- Wie gehen Fertigungsunternehmen mit aktuellen und zukünftigen Bedrohungslagen um
- Bedrohungsherausforderungen und Sicherheitslücken in der Fertigungsindustrie
- Prioritäten und Pläne für die Einführung neuer Technologien, die Anpassung an Rahmenbedingungen und die Behebung von Qualifikationslücken

Wichtigste Erkenntnisse:

- Mehr als 38 % aller Fertigungsunternehmen erleiden Umsatzeinbußen in Höhe von 20 bis 50 Millionen US-Dollar, sobald ihre Active Directory-Umgebung 24 Stunden lang kompromittiert wird. 32 % davon erleiden hingegen Verluste zwischen 50 und 100 Millionen US-Dollar
- Die Industriespionage (21 %) sowie Ransomware (22 %) zählen zu den größten Sicherheitsbedrohungen in der Fertigungsindustrie
- 33 % aller Fertigungsunternehmen halten Cybersicherheit zwar für wichtig, verlassen sich aber dennoch bei der Einführung neuer Technologien nur auf die bereits vorhandene Sicherheit, ohne diese zusätzlich zu überprüfen
- 80 % Prozent aller Befragten geben an, dass die Cybersicherheit ihres Unternehmens durch den Fachkräftemangel negativ beeinflusst wurde
- Mehr als die Hälfte der Befragten (54 %) hält Cybersicherheit bei der Einführung neuer Technologien für wichtig
- Zwei Drittel der Befragten (66 %) sind der Meinung, dass sich das Potenzial von Cybersicherheitsrisiken negativ auf die Geschwindigkeit der Einführung neuer Technologien in ihrem Unternehmen auswirken wird
- Die überwältigende Mehrheit (87 %) gibt an, dass ihre Cybersicherheitsmaßnahmen mit dem NIST-Framework übereinstimmen
- Mehr als zwei Drittel der Befragten (67 %) geben an, dass die Ausrichtung auf ein Cybersicherheits-Framework für ihr Unternehmen eine mittlere bis hohe Priorität hat
- Bei der Beurteilung, ob die Cybersicherheit eines Unternehmens durch einen Fachkräftemangel negativ beeinflusst wurde, gaben vier Fünftel der Befragten an, negativ betroffen zu sein (80 %)
- Das schnelle Tempo der Einführung neuer Technologien (33 %) wurde als die größte Herausforderung für Unternehmen bei der Qualifikationslücke im Bereich der Cybersicherheit genannt, dicht gefolgt von der Abhängigkeit von Legacy-Technologien (27 %) und Budgetbeschränkungen (27 %)

Quest

priorities

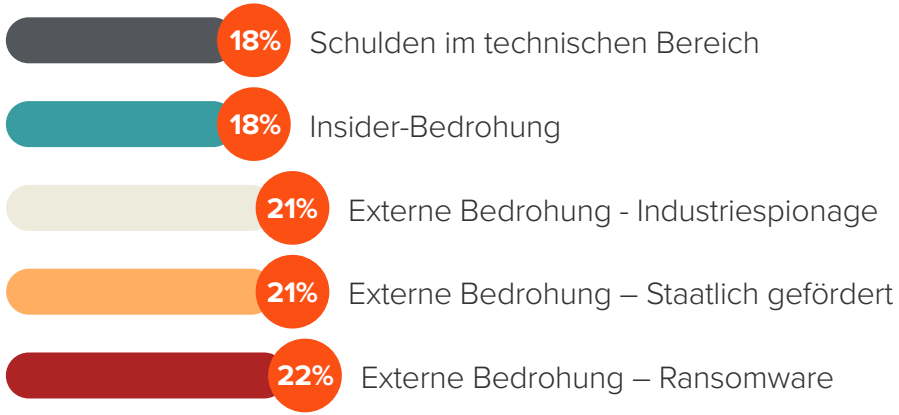
A Lynchpin Media BRAND

TEIL 1:

Herausforderungen bei der Cybersicherheit in der Fertigungsindustrie

Die Bewältigung zunehmender Cyberangriffe und die Abstimmung von Cybersicherheitsmaßnahmen mit organisatorischen Rahmenbedingungen gilt für viele Fertigungsunternehmen als zentrales Anliegen. In diesem Abschnitt untersuchen wir die Bedrohungslage der Branche sowie die größten Herausforderungen für die Befragten beim Schutz ihres Angriffswegs.

Aus was bestehen Ihrer Meinung nach die größten Sicherheitsbedrohungen in der Fertigungsindustrie? (Bitte wählen zwei Optionen aus)



Schlussfolgerung

Ransomware (22 %), Industriespionage (21 %) sowie staatlich geförderte Bedrohungen (21 %) gelten als die größten Sicherheitsbedrohungen in der Fertigungsindustrie. Also eine klare Darstellung des aktuellen Zustands der Angriffslage und der Notwendigkeit für Fertigungsunternehmen, die OT-Sicherheit so früh wie möglich zu berücksichtigen.

Quest

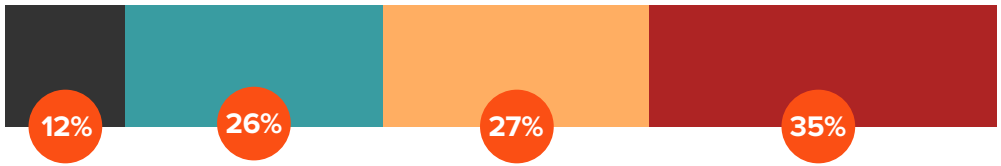
priorities

A Lynchpin Media BRAND

TEIL 1:

Herausforderungen bei der Cybersicherheit in der Fertigungsindustrie

Welchen der folgenden Vorfälle haben Sie in Ihrem Unternehmen selbst miterlebt? (Bitte wählen Sie zwei Optionen aus)



- Unbeabsichtigtes Datenleck (Laptop an die falsche Person geschickt usw.)
- Diebstahl von Zugangsdaten/Kompromittierung von Konten
- Phishing/Social Engineering
- Ransomware/Malware

Schlussfolgerung

Die Befragten geben an, dass Ransomware/Malware (35 %) und Phishing/Social Engineering (27 %) ihre erfahrensten Angriffsformen sind. Dies unterstreicht die dringende Notwendigkeit, eine mehrschichtige Sicherheit gegen gezielte und dateilose Angriffe aufzubauen, die Viren, Spyware, Malware und Ransomware stoppen können. Besorgniserregend ist aber dennoch, dass das verarbeitende Gewerbe zu den fünf Branchen gehört, in denen Cyberangriffe am häufigsten vorkommen, was natürlich die Notwendigkeit mehrerer leistungsstarker Schutzebenen erfordert.

Quest

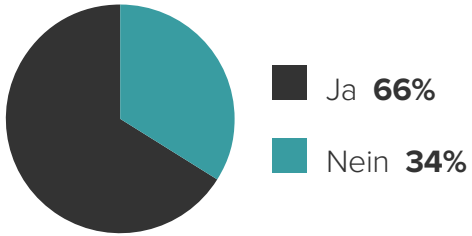
priorities

A Lynchpin Media BRAND

TEIL 1:

Herausforderungen bei der Cybersicherheit in der Fertigungsindustrie

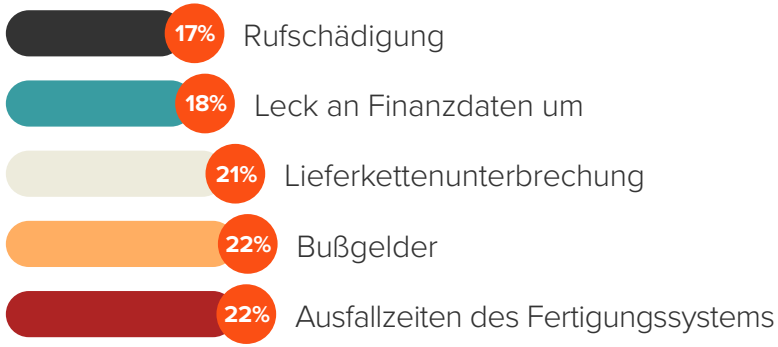
Glauben Sie, dass Ihr Unternehmen innerhalb der nächsten 12 Monate Ziel eines Cyberangriffs sein könnte?



Schlussfolgerung

Mehr als die Hälfte aller Befragten (66 %) ist der Meinung, dass ihr Fertigungsunternehmen innerhalb der nächsten 12 Monate Ziel eines Cyberangriffs werden könnte. Dies verdeutlicht die Tatsache, dass Angreifer, solange die Digitalisierung weiterhin voranschreitet, immer mehr neue Wege finden werden, um industrielle Steuerungssysteme ins Visier zu nehmen, so dass die Sicherheit für Unternehmen in Zukunft entweder eine hohe oder mittlere Priorität haben sollte.

Welches der folgenden Probleme ist Ihnen am wichtigsten, um es mit Cybersicherheitsmaßnahmen zu entschärfen? (Bitte wählen Sie zwei Optionen aus)



Schlussfolgerung

Ausfallzeiten von Fertigungssystemen (22 %) und Bußgelder (22 %) sind für Fertigungsunternehmen die besorgniserregendsten Bereiche, wenn es darum geht, Cybersicherheitsrisiken zu mindern. Da diese Organisationen Projekte und die damit verbundenen Risiken überwachen, sind belastbare Sicherheitstools von entscheidender Bedeutung, um die Abwehr zu stärken. Dies bedeutet auch, dass die Sicherheitsbudgets wahrscheinlich angepasst werden müssen, um diesen Problembereichen Rechnung zu tragen.

Quest

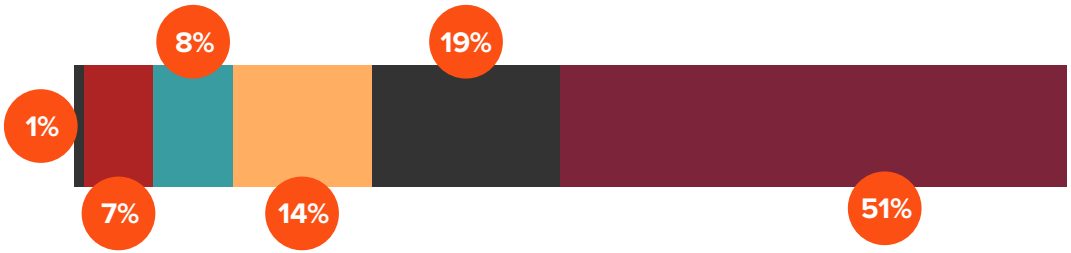
priorities

A Lynchpin Media BRAND

TEIL 1:

Herausforderungen bei der Cybersicherheit in der Fertigungsindustrie

Wie oft überprüfen Sie die Schwachstellen und potenziellen Angriffswege, die derzeit in Ihrer Active Directory-Umgebung vorhanden sind?



- Wir tun dies nicht
- Ich weiß nicht
- Wöchentlich
- Jährlich
- Monatlich
- Alle 6 Monate

Schlussfolgerung

Mehr als die Hälfte aller Befragten (51 %) gibt an, dass die Routine zur Überprüfung von Schwachstellen und potenziellen Angriffspfaden innerhalb ihrer Active Directory-Umgebung nur zweimal im Jahr vorkommt. Nur 19 % führen monatliche und 7 % wöchentliche Überprüfungen durch. In Anbetracht der rasanten Expansion der Bedrohungslage und der Tatsache, dass Überprüfungen ausnutzbare Pfade aufdecken, wird dringend empfohlen, dass Unternehmen mehr Sicherheitsmitarbeiter einstellen, die wichtige Assets stets überprüfen und schützen können.

Quest

priorities

A Lynchpin Media BRAND

TEIL 1:

Herausforderungen bei der Cybersicherheit in der Fertigungsindustrie

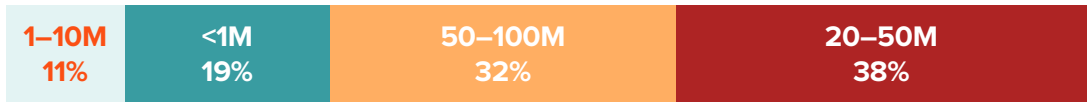
Sollten Sie geantwortet haben “Wir tun das nicht” - Warum führen Sie dann derzeit immer noch keine Überprüfung durch?

- Mangelndes Fachwissen **50%**
- Mangel an adäquaten Tools/Lösungen **50%**

Schlussfolgerung

Mangelndes Fachwissen (50 %) und das Fehlen geeigneter Tools und Lösungen (50 %) zählen zu den Hauptgründen, warum einige Fertigungsunternehmen Schwachstellen und potenzielle Angriffswege, die derzeit in ihrer Active Directory-Umgebung vorhanden sind, nicht überprüfen. Sollte der weltweite Mangel an Cyber-Fachkräften und adäquaten Tools anhalten, wird es für Unternehmen immer schwieriger, auf der Gewinnerseite des Sicherheitskampfes zu stehen. Zufolge wird dies den Fortschritt bei der Erzielung eines angemessenen und wirksamen Schutzes im Produktionsprozess eindeutig bremsen.

Wie hoch wäre der geschätzte Umsatzverlust Ihres Unternehmens, wenn Ihre Active Directory-Umgebung für 24 Stunden kompromittiert werden würde?



Schlussfolgerung

Sollte die Active Directory-Umgebung eines Fertigungsunternehmens für 24 Stunden kompromittiert werden, verlieren ganze 38 % dieser Unternehmen einen geschätzten Umsatz von 20 bis 50 Millionen US-Dollar, während 32 % einen Verlust von 50 bis 100 Millionen US-Dollar erleiden. Umgekehrt würden Unternehmen, die dazu bereit wären, einen proaktiveren Anlageansatz für ihre Sicherheitslage zu verfolgen, in so einem Fall Millionen einsparen. Es ist auch sehr unwahrscheinlich, vorherzusagen, dass eine kompromittierte Active Directory-Umgebung nur 24 Stunden andauern wird. Dies bedeutet, dass Investitionen in Sachen Sicherheit nur eine Aufwärtsspirale und ein strategischer Schritt in die richtige Richtung für Unternehmen wären, um mehr zu sparen.

Quest

priorities

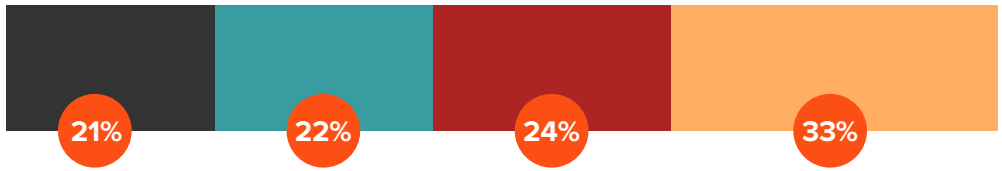
A Lynchpin Media BRAND

TEIL 2:

Prioritäten und Pläne für die Einführung neuer Technologien, die Anpassung an die Rahmenbedingungen sowie die Behebung von Qualifikationslücken

Investitionen und die Anpassung an neue Technologien sind entscheidend, um der aktuellen Zunahme von Angriffen zu begegnen. In diesem Abschnitt befassen wir uns mit den wichtigsten Überlegungen für Unternehmen im kommenden Jahr und wie ihre notwendigsten Prioritäten aussehen.

Wie wichtig ist Cybersicherheit bei der Einführung neuer Technologien?



- Wir können Cybersicherheit zwar in Betracht ziehen, betrachten sie aber in den meisten Szenarien dennoch nur als optional
- Wir halten es nicht für wichtig
- Wir führen jedes Mal, wenn eine neue Technologie eingeführt wird, eine spezielle Überprüfung der Cybersicherheit durch
- Wir halten es für wichtig, vertrauen aber in den meisten Fällen einfach unserer bestehenden Cybersicherheit ohne zusätzliche Überprüfungen

Schlussfolgerung

Mehr als die Hälfte aller Befragten (57 %) hält Cybersicherheit für wichtig, wenn es um die Einführung neuer Technologien geht. Fast ein Viertel der Befragten (24 %) gibt an, dass sie bei jeder Einführung einer neuen Technologie immer eine spezielle Überprüfung der Cybersicherheit durchführen. Dies zeigt also deutlich, dass die Einführung innovativer Technologien eine entscheidende Komponente ist und auch immer sein wird, um Unternehmen in die Lage zu versetzen, ihre Sicherheitslage zu stärken. Wir beobachten aber trotzdem immer noch, dass ein großer Teil der Unternehmen ihrer bestehenden Cybersicherheit ohne zusätzliche Überprüfungen vertraut, was natürlich Chancen für Anbieter bietet, die sich darauf spezialisiert haben, größere Angriffsflächen vor der Einführung digitaler Technologien zu schützen.

Quest

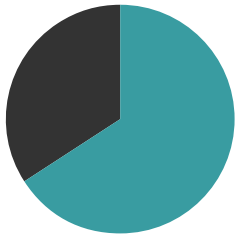
priorities

A Lynchpin Media BRAND

TEIL 2:

Prioritäten und Pläne für die Einführung neuer Technologien, die Anpassung an die Rahmenbedingungen sowie die Behebung von Qualifikationslücken

Denken Sie, dass sich das Potenzial von Cybersicherheitsrisiken negativ auf die Geschwindigkeit der Einführung neuer Technologien in Ihrem Unternehmen auswirken wird?



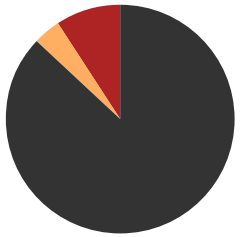
Ja **66%**

Nein **34%**

Schlussfolgerung

Zwei Drittel der Befragten (66 %) sind der Meinung, dass sich das Potenzial von Cybersicherheitsrisiken negativ auf die Geschwindigkeit der Einführung neuer Technologien in ihrem Unternehmen auswirken wird. Unternehmen sollten daher in diese Bereiche investieren, um ihre Netzwerke zu schützen und angemessen auf Disaster-Recovery-Situationen vorbereitet zu sein. Dies unterstreicht die Notwendigkeit für Sicherheitspartner, diese Sicherheitspläne umzusetzen und diesen Unternehmen dabei zu helfen, neue Technologien schneller einzuführen.

Stehen Ihre Cybersicherheitsmaßnahmen im Einklang mit dem NIST-Framework?



Ja **87%**

Nein **4%**

Wir haben noch nie etwas von NIST **9%**

Schlussfolgerung

Die überwältigende Mehrheit (87 %) gibt an, dass ihre Cybersicherheitsmaßnahmen mit dem NIST-Framework übereinstimmen. Aus Sicht der IT und der Cybersicherheit sollte die Einhaltung des NIST-Frameworks für Unternehmen, die den Wert der Einhaltung gesetzlicher Vorschriften verstehen, oberste Priorität haben. Unternehmen benötigen daher Sicherheitspartner, die die ordnungsgemäße Umsetzung des NIST-Rahmenansatzes leiten können.

Quest

priorities

A Lynchpin Media BRAND

TEIL 2:

Prioritäten und Pläne für die Einführung neuer Technologien, die Anpassung an die Rahmenbedingungen sowie die Behebung von Qualifikationslücken

Mit Blick auf die nächsten 12 Monate, welche Priorität wird die Ausrichtung auf ein Cybersicherheits-Framework für Ihr Unternehmen haben?

Niedrige Priorität. Wir priorisieren OT nicht, indem wir uns an einem Cybersicherheits-Framework orientieren

Mittlere Priorität. . Wir müssen Schritte unternehmen, um besser aufeinander abgestimmt zu sein, aber wir müssen dies auch gegen andere Sicherheitsziele abwägen.

Hohe Priorität. Wir besitzen schon jetzt viel mehr vernetzte Geräte und damit viel mehr Risiken – ein hohes Maß an Ausrichtung zu erreichen, ist zu einem strategischen Ziel geworden

Schlussfolgerung

Mehr als zwei Drittel aller Befragten (67 %) geben an, dass die Ausrichtung auf ein Cybersicherheits-Framework für ihr Unternehmen eine mittlere bis hohe Priorität darstellt. Dies deutet also darauf hin, dass Unternehmen in kritische Infrastrukturen investieren müssen, um ein ständig wachsendes Ökosystem vernetzter Geräte zu unterstützen und ein Gleichgewicht zwischen strategischen und Sicherheitszielen zu erreichen. Es zeigt außerdem, dass Unternehmen nach unvoreingenommenen, überlegenen Cybersicherheitslösungen suchen und eine langfristige Risikomanagementstrategie verfolgen, die ihre Sicherheitslage unterstützt.

Quest

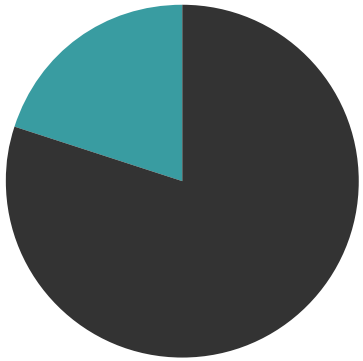
priorities

A Lynchpin Media BRAND

TEIL 2:

Prioritäten und Pläne für die Einführung neuer Technologien, die Anpassung an die Rahmenbedingungen sowie die Behebung von Qualifikationslücken

Wurde die Cybersicherheit Ihres Unternehmens bereits durch einen Fachkräftemangel negativ beeinflusst?



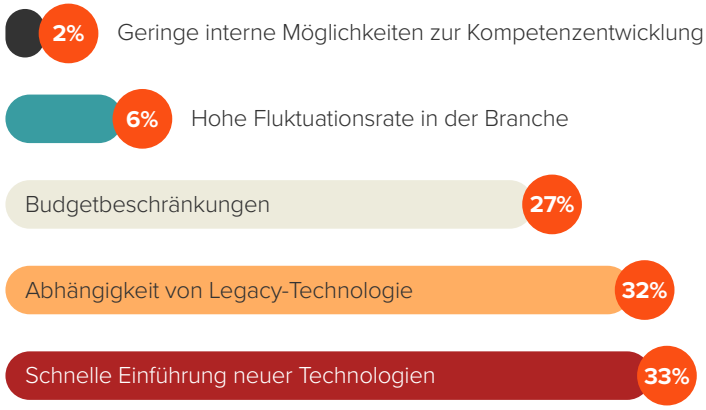
Ja **80%**

Nein **20%**

Schlussfolgerung

Bei der Beurteilung, ob die Cybersicherheit eines Unternehmens durch einen Fachkräftemangel negativ beeinflusst wurde, gaben vier Fünftel der Befragten an, negativ betroffen zu sein (80 %). Hier gibt es Argumente für einen vertrauenswürdigen Sicherheitsanbieter, der eine Lückenanalyse durchführen kann, um Wachstumschancen zu identifizieren und Ressourcen zu priorisieren. Wenn diese Qualifikationslücke aber nicht geschlossen wird, wird sich die Ineffizienz am Arbeitsplatz verschärfen, da die Mitarbeiter Schwierigkeiten damit haben werden, ihre Aufgaben zu bewältigen und zugewiesene Aufgaben zu erfüllen. Und da die Produktivität im Mittelpunkt von Fertigungsprozessen steht, würde eine Analyse der Qualifikationslücken dazu beitragen, die Gesamteffizienz zu bewerten und besser auf Cyberangriffe vorbereitet zu sein.

Aus was besteht die größte Herausforderung bei der Qualifikationslücke im Bereich Cybersicherheit, mit der Ihr Unternehmen konfrontiert ist?



Schlussfolgerung

Das schnelle Tempo der Einführung neuer Technologien (33 %) wurde als die größte Herausforderung für Unternehmen bei der Qualifikationslücke im Bereich der Cybersicherheit genannt, dicht gefolgt von der Abhängigkeit von Legacy-Technologien (27 %) und Budgetbeschränkungen (27 %). Dies deutet darauf hin, dass Unternehmen mit Anbietern zusammenarbeiten sollten, die dazu beitragen können, eine Sicherheitskultur zu vermitteln, die die Einführung von Technologien optimiert und Angebote zu komfortablen Preisen bietet. Unternehmen sollten erwägen, in Cybersicherheitsschulungen und die Aktualisierung von Legacy-Technologien zu investieren, damit sich jeder potenzieller Warnsignale bewusst ist, wenn es darum geht, seine Daten und Kollegen zu schützen.

Quest

priorities

A Lynchpin Media BRAND

ABSCHLUSS

Da die Mehrheit der Befragten angab, dass die Ausrichtung auf ein Cybersicherheits-Framework für ihre Unternehmen im nächsten Jahr eine mittlere bis hohe Priorität hat, gibt es keinen besseren Zeitpunkt, um in Cybersicherheitspartner zu investieren, die sich auf eine langfristige Resilienz konzentrieren und über Erfahrung bei der Begrenzung von Bußgeldern verfügen. Die Folgen eines Mangels an Cybersicherheitsfachkräften können für ein Unternehmen sehr schädlich sein und angesichts der Tatsache, dass übersehene Bedrohungen die Hauptfolge daraus sind, ist eine Investition in Schulungen unerlässlich. Und da Unternehmen ihre Angriffsfläche aufgrund der Einführung digitaler Technologien reduzieren möchten, ist dies eine hervorragende Gelegenheit für Anbieter, einen umfassenden Ansatz für die Modernisierung von Active Directory-Umgebungen und Innovationen anzubieten. Da jedoch ein höherer Prozentsatz der Befragten der Meinung ist, dass sich das Potenzial von Cybersicherheitsrisiken negativ auf die Geschwindigkeit der Einführung neuer Technologien auswirken wird, müssen Anbieter einen komfortablen Preis anbieten, der es Unternehmen ermöglicht, maximalen Nutzen zu erzielen.

Ein weiterer Problembereich war aber auch die Sicherstellung, dass Unternehmen über die entsprechenden Sicherheitsvorkehrungen verfügen, um Systemausfälle und Unterbrechungen der Lieferkette zu bekämpfen. Die Ergebnisse zeigen, dass Ransomware, Malware, Phishing und Social Engineering die größten Probleme von Unternehmen sind. Durch einen langfristigen Ansatz sowie die Sicherung eines vertrauenswürdigen Partners, der ihnen dabei hilft, eine proaktive Strategie für Technologie und Innovation zu entwickeln, können sich Unternehmen auf den Weg zu einer verbesserten Cyber-Resilienz machen. Die Fertigungsindustrie ist also mit großen Unsicherheiten behaftet und einen Partner zu haben, der über Erfahrung im Bereich Disaster Recovery verfügt, würde einen erheblichen Vorteil für den Aufbau eines sicherheitsweiten Ethos bieten.

DA UNTERNEHMEN IHRE ANGRIFFSFLÄCHE AUFGRUND DER EINFÜHRUNG DIGITALER TECHNOLOGIEN REDUZIEREN MÖCHTEN, STELLT DIES EINE HERVORRAGENDE GELEGENHEIT FÜR ANBIETER DAR, EINEN UMFASSENDEN ANSATZ FÜR DIE MODERNISIERUNG VON ACTIVE DIRECTORY-UMGEBUNGEN UND INNOVATIONEN ANZUBIETEN.

Lynchpin Media ist ein globales Unternehmen für Technologiemedien, Daten und Marketingdienstleistungen. Wir helfen dabei, das Bewusstsein zu schärfen, Schlüsselkunden zu entwickeln und gezielt anzusprechen und wichtige Informationen über regionale Trends zu erfassen. Besuchen **lynchpinmedia.com** für mehr Informationen.

CxO Priorities, eine Lynchpin-Medienmarke

63/66 Hatton Garden
London, EC1N 8LE

Finde mehr heraus: **www.cxopriorities.com**

Gefördert durch

Quest