ARTUS GRUPPE

MARCUS UNGER

/ CYBER-VERSICHERUNG

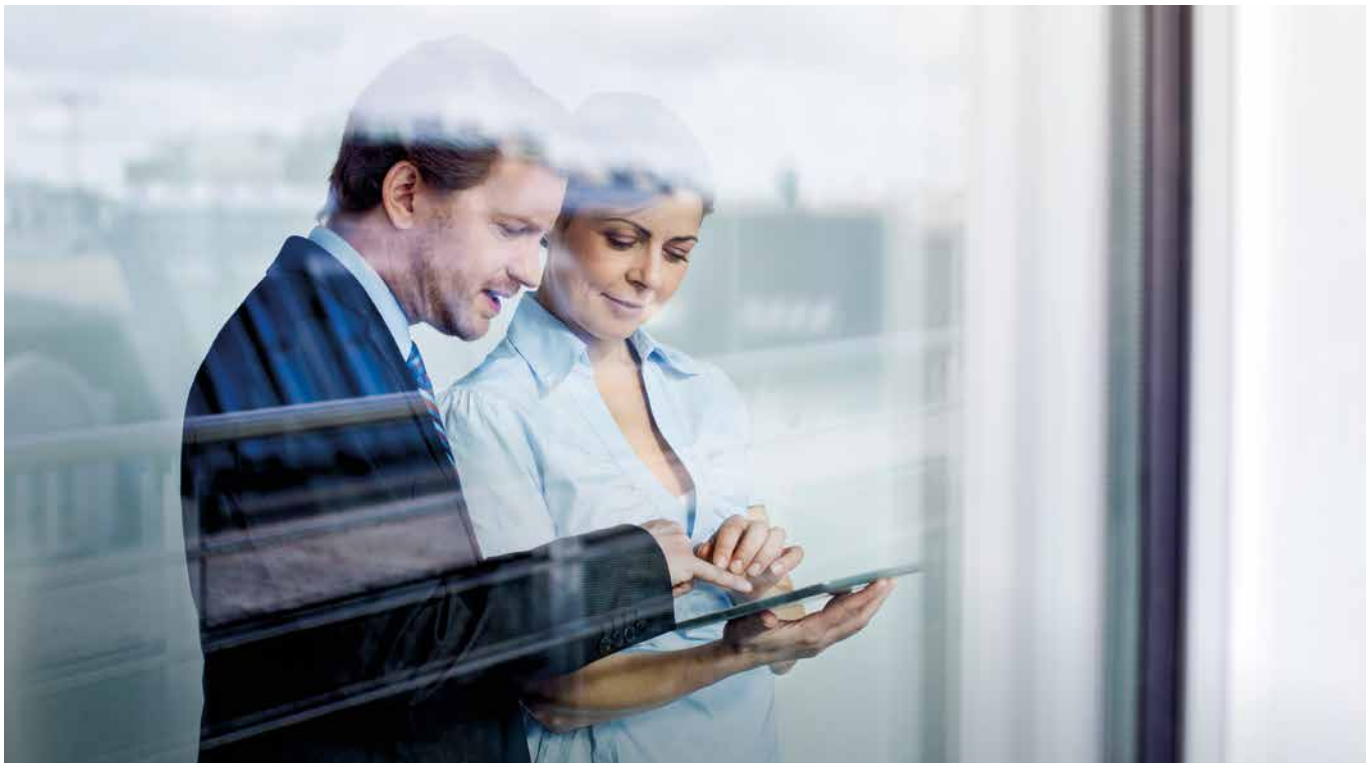
SCHLÜSSIGE ÜBERLEBENSSTRATEGIEN FÜR DEN MITTELSTAND

INHALT

Cyber-Angriffe sind real. Nicht ohne Grund gehören sie zu den größten Risiken eines mittelständischen Unternehmens. Wir dürfen uns nicht mehr fragen, ob wir Opfer eines Angriffes werden, sondern viel mehr wann. Gerade durch die raschen Entwicklungsschritte der letzten Jahre im Bereich der Digitalisierung, ist auch die Cyberkriminalität gestiegen. Das unterstreicht die Dringlichkeit, geeignete Maßnahmen zu ergreifen – nur, wer eine gute Cybersecurity hat, ist in Zukunft gut aufgestellt hat. Dieses Dossier beleuchtet, wie der Mittelstand effektiv Cyber-Gefahren begegnen und sich gegen potenzielle Bedrohungen wappnen kann.

I. **RISIKEN IDENTIFIZIEREN UND BEWERTEN** /

Die Grundlage jeglicher Maßnahmen zur Erhöhung der IT-Sicherheit in Unternehmen bildet eine umfassende Bestandsaufnahme der vorhandenen technischen und organisatorischen Sicherheitsvorkehrungen. Dieser erste, entscheidende Schritt ermöglicht es, eine klare Übersicht über den aktuellen Stand der IT-Sicherheit zu erhalten und potenzielle Schwachstellen sowie Optimierungspotenziale zu identifizieren. Die technische Sicherheit umfasst dabei sämtliche hardware- und softwarebasierten Mechanismen, die dazu dienen, die IT-Infrastruktur vor unerlaubten Zugriffen, Ausfällen und anderen Sicherheitsbedrohungen zu schützen. Hierzu zählen unter anderem Firewalls, Verschlüsselungstechnologien, Zugriffskontrollsysteme und regelmäßige Sicherheitsupdates. Im Gegensatz dazu bezieht sich die organisatorische Sicherheit auf die in einem Unternehmen etablierten Prozesse, Richtlinien und Verfahren, die das sichere Arbeiten mit IT-Systemen gewährleisten sollen. Dazu gehören beispielsweise Richtlinien zur Passwortvergabe, zum Umgang mit sensiblen Daten oder zur regelmäßigen Durchführung von Awareness-Schulungen für Mitarbeiter.



Um im Falle eines Sicherheitsvorfalls adäquat reagieren zu können, ist es zudem unerlässlich, potenzielle Schadenszenarien im Vorfeld zu definieren und entsprechende Überlebensstrategien zu entwickeln. Hierbei geht es um die Frage, wie im schlimmsten anzunehmenden Fall, verfahren werden soll, um den Schaden möglichst gering zu halten und den Fortbestand des Unternehmens zu sichern. Ein fundierter Notfallplan, der genau festlegt, welche Schritte in einem solchen Szenario unternommen werden müssen, ist dabei von zentraler Bedeutung. Darüber hinaus ist die Einrichtung eines Krisenstabes empfehlenswert, der im Ernstfall die Koordination der erforderlichen Maßnahmen übernimmt und als zentrale Anlaufstelle für alle Beteiligten dient.

Eine weitere wesentliche Komponente der Überlebensstrategie stellt das Konzept der Business Continuity dar. Dieses zielt darauf ab, kritische Geschäftsprozesse auch unter widrigen Umständen aufrechtzuerhalten bzw. schnellstmöglich wiederherzustellen. Dazu gehört die Entwicklung eines Wiederanlaufplans, der detailliert beschreibt, in welcher Reihenfolge und innerhalb welcher Zeitspanne die verschiedenen Geschäftsprozesse nach einem Vorfall wieder aufgenommen werden sollen.

Dieser Plan ist entscheidend, um nach einem Sicherheitsvorfall den Betrieb zügig wieder aufnehmen zu können und so langfristige Schäden für das Unternehmen zu vermeiden. Insgesamt zeigt sich, dass eine umfassende Bestandsaufnahme der IT-Sicherheit in Unternehmen den Grundstein für die Entwicklung einer effektiven Sicherheitsstrategie legt. Indem sowohl technische als auch organisatorische Aspekte berücksichtigt werden, potenzielle Schadenszenarien durchdacht und entsprechende Notfall- und Wiederanlaufpläne erstellt werden, können Unternehmen sich auf mögliche Sicherheitsvorfälle vorbereiten und so ihre Resilienz gegenüber Cyber-Bedrohungen signifikant erhöhen.

II. **BEWUSSTSEIN SCHAFFEN DURCH SCHULUNGEN /**

Der menschliche Faktor spielt bei Cyber-Angriffen eine wesentliche Rolle. Phishing-E-Mails, unsichere Passwörter oder die fahrlässige Handhabung von sensiblen Daten können schnell zum Einfallstor für Cyber-Kriminelle werden. Umso wichtiger ist es, das Bewusstsein für Cyber-Sicherheit bei allen Mitarbeitern zu schärfen. Regelmäßige Awareness-Schulungen, die über aktuelle Gefahren informieren und den sicheren Umgang mit digitalen Ressourcen vermitteln, sind hierbei unerlässlich. Solche Schulungen tragen dazu bei, das Risiko von Sicherheitsvorfällen durch menschliches Versagen signifikant zu reduzieren.

||| BACKUP UND WIEDERHERSTELLUNG /

Eine effektive Methode, um die Resilienz gegenüber Cyber-Angriffen zu erhöhen, ist die regelmäßige Sicherung wichtiger Daten. Backups gewährleisten, dass im Falle eines Cyber-Angriffs, wie beispielsweise einer Ransomware-Attacke, die Daten schnell wiederhergestellt und der Geschäftsbetrieb aufrechterhalten werden kann. Wichtig ist dabei, die Backups getrennt vom Netzwerk zu speichern, um zu verhindern, dass sie ebenfalls kompromittiert werden.

In der modernen Unternehmenswelt, in der Daten oft als das neue Gold betrachtet werden, ist nicht allein die Existenz von Backups von entscheidender Bedeutung, sondern vielmehr die Fähigkeit, diese Daten im Notfall auch erfolgreich wiederherzustellen. Die effektive Wiederherstellung von Unternehmensdaten nach einem Datenverlust, sei es durch Cyberangriffe, technische Defekte oder menschliche Fehler, ist zentral für die Aufrechterhaltung des Betriebs und die Minimierung von Ausfallzeiten und damit verbundenen Kosten. Daher ist es nicht ausreichend, lediglich Backups anzulegen; Unternehmen müssen vielmehr sicherstellen, dass diese Backups auch eine verlässliche Quelle für die Wiederherstellung der betrieblichen Daten darstellen. In diesem Zusammenhang kommt Offline-Backups eine besondere Bedeutung zu. Da sie nicht permanent mit dem Netzwerk verbunden sind, bieten sie einen zusätzlichen Schutz vor Ransomware und anderen Cyber-Bedrohungen, die darauf abzielen, nicht nur primäre Datenbestände, sondern auch deren Sicherungskopien zu kompromittieren.

Die Isolierung von Offline-Backups stellt somit eine zusätzliche Sicherheitsebene dar, die es ermöglicht, selbst in Fällen, in denen die primären und online gespeicherten Sicherungen angegriffen wurden, eine zuverlässige Datenwiederherstellung durchzuführen. Des Weiteren ist die Führung einer Historie von Backups, die es erlaubt, auf verschiedene, zeitlich zurückliegende Datenstände zuzugreifen, unerlässlich. Dies ist besonders relevant, wenn Daten nicht sofort nach ihrer Beschädigung oder Löschung wiederhergestellt werden müssen oder können, oder wenn Fehler erst nach einiger Zeit entdeckt werden. Eine solche Historie ermöglicht es, auf ältere, unversehrte Versionen der Daten zurückzugreifen und so einen Zustand vor dem Datenverlust wiederherzustellen. Die Möglichkeit, zu einem spezifischen Zeitpunkt in der Vergangenheit zurückzukehren, kann auch bei der Bewältigung von Datenkorruption, die über längere Zeiträume unbemerkt blieb, von unschätzbarem Wert sein.

Allerdings nützt die beste Backup-Strategie wenig, wenn nicht regelmäßig überprüft wird, ob die Wiederherstellung der Daten aus den Backups auch erfolgreich und in einem akzeptablen Zeitrahmen durchgeführt werden kann. Regelmäßige Tests der Wiederherstellungsprozesse sind daher unerlässlich,

HANDLUNGS-EMPFEHLUNGEN /

- Identifizieren Sie in einem strukturierten Prozess möglichst alle Cyber-Risiken und bewerten diese
- Kümmern Sie sich nicht nur um die technische Sicherheit, sondern auch besonders um die organisatorische Sicherheit
- Testen Sie den Ernstfall und wiederholen Sie solche Tests regelmäßig

um sicherzustellen, dass im Ernstfall die benötigten Daten effektiv und schnell zur Verfügung stehen. Solche Tests helfen nicht nur, die Funktionalität des Wiederherstellungsprozesses zu verifizieren, sondern bieten auch die Möglichkeit, die Dauer der Wiederherstellung realistisch einzuschätzen und gegebenenfalls Optimierungen vorzunehmen. Durch das regelmäßige Durchspielen von Wiederherstellungsszenarien können Unternehmen zudem sicherstellen, dass die Verantwortlichen im Umgang mit den Backup- und Wiederherstellungswerkzeugen geübt sind und im Notfall schnell und effizient handeln können.

IV. **AWARENESS-SCHULUNGEN ERHÖHEN DAS IT-SICHERHEITSNIVEAU DEUTLICH /**

Awareness-Schulungen spielen eine zentrale Rolle im Rahmen der Cyber-Sicherheitsstrategie eines Unternehmens, da sie direkt auf den menschlichen Faktor abzielen, der oft als das schwächste Glied in der Sicherheitskette betrachtet wird.

Die zunehmende Komplexität und Raffinesse von Cyber-Angriffen, insbesondere solche, die auf Social Engineering und Phishing-Techniken setzen, machen es unerlässlich, dass jeder Mitarbeiter, nicht nur das IT-Personal, ein grundlegendes Verständnis von Cyber-Risiken und den Best Practices zum Schutz sensibler Informationen besitzt. Awareness-Schulungen zielen darauf ab, dieses Bewusstsein zu schärfen und eine Kultur der Cyber-Sicherheit im gesamten Unternehmen zu etablieren, in der Sicherheitsrichtlinien nicht nur bekannt sind, sondern auch aktiv gelebt werden. Versicherer legen auf Awareness-Schulungen besonderen Wert, da ein gut informierter und sensibilisierter Mitarbeiterstamm das Risiko signifikanter Sicherheitsvorfälle erheblich reduzieren kann. Unternehmen, die in die Aus- und Weiterbildung

ihrer Mitarbeiter in Bezug auf Cyber-Sicherheit investieren, demonstrieren ein proaktives Risikomanagement, das nicht nur die Wahrscheinlichkeit und das Ausmaß von Schadensfällen verringert, sondern auch dazu beiträgt, die Kosten für Cyber-Versicherungspolicen zu optimieren. Versicherer erkennen solche Unternehmen oft als geringeres Risiko an, da die Chance auf erfolgreiche Cyber-Angriffe durch das erhöhte Sicherheitsbewusstsein der Mitarbeiter reduziert wird.

Darüber hinaus sind Awareness-Schulungen ein wesentliches Element, um die Einhaltung gesetzlicher und regulatorischer Anforderungen, wie beispielsweise der Datenschutz-Grundverordnung (DSGVO), sicherzustellen. Verstöße gegen Datenschutzbestimmungen können nicht nur zu erheblichen finanziellen Strafen führen, sondern auch den Ruf eines Unternehmens nachhaltig schädigen. Durch regelmäßige Schulungen, die Mitarbeiter über ihre Pflichten und Verantwortlichkeiten im Umgang mit personenbezogenen Daten aufklären, minimieren Unternehmen das Risiko rechtlicher Konsequenzen und stärken gleichzeitig das Vertrauen ihrer Kunden und Geschäftspartner.

Letztendlich reflektieren Awareness-Schulungen die Erkenntnis, dass technische Sicherheitsmaßnahmen allein nicht ausreichen, um die Cybersicherheit eines Unternehmens zu gewährleisten. Die menschliche Komponente muss als integraler Bestandteil der Sicherheitsstrategie betrachtet werden. Durch die kontinuierliche Weiterbildung und Sensibilisierung der Mitarbeiter tragen Unternehmen nicht nur zu einem sichereren Arbeitsumfeld bei, sondern positionieren sich auch als verantwortungsbewusste und attraktive Partner für Versicherer, was letztlich zu besseren Konditionen bei der Absicherung von Cyber-Risiken führen kann.

V. **SECURITY OPERATIONS CENTER (SOC) /**

Für Unternehmen, die ihre IT-Sicherheit auf das nächste Level heben möchten, bietet sich die Einrichtung eines Security Operations Center (SOC) an. Ein SOC überwacht kontinuierlich die IT-Infrastruktur auf Sicherheitsvorfälle, analysiert potenzielle Bedrohungen und reagiert umgehend auf identifizierte Gefahren.

Für KMUs, für die ein eigenes SOC wirtschaftlich nicht darstellbar ist, bieten sich Dienstleistungen von externen Anbietern an, die ein SOC-as-a-Service bereitstellen. Dies ermöglicht auch kleineren Unternehmen den Zugang zu professionellen Sicherheitsmechanismen.

In der heutigen, global vernetzten Geschäftswelt ist die Bedrohung durch Cyberangriffe omnipräsent und kennt keine Grenzen. Angreifer agieren aus allen Teilen der Welt und nutzen die Tatsache, dass Unternehmen nicht zu jeder Zeit ihre

IT-Systeme überwachen können. Diese kontinuierliche und komplexe Bedrohungslage unterstreicht die Notwendigkeit einer rund um die Uhr stattfindenden Überwachung der IT-Sicherheit, wie sie ein Security Operations Center (SOC) bietet. Ein SOC übernimmt genau diese Aufgabe: Es überwacht kontinuierlich die Sicherheitslage, analysiert Sicherheitswarnungen und reagiert umgehend auf potenzielle Bedrohungen. Die Herausforderung dabei ist, dass die Flut an Sicherheitsmeldungen, die täglich generiert werden, so umfangreich ist, dass eine manuelle Sichtung und Analyse durch Mitarbeiter einer IT-Abteilung kaum möglich ist. Diese Realität macht die Etablierung eines eigenen, unternehmensinternen SOC für viele Unternehmen, insbesondere für kleine und mittelständische, zu einer kostenintensiven und ressourcenaufwendigen Angelegenheit.

Vor diesem Hintergrund bietet der Einkauf einer SOC-Dienstleistung eine praktikable und effiziente Lösung. Externe Dienstleister, die sich auf die Bereitstellung von SOC-Services spezialisiert haben, verfügen über die notwendige Expertise und technologische Ausstattung, um die IT-Sicherheit von Unternehmen kontinuierlich zu überwachen und zu verbessern. Eine solche Auslagerung ermöglicht es Unternehmen, von den Vorteilen eines SOC zu profitieren, ohne selbst die enormen Investitionen in Technologie und Fachpersonal tätigen zu müssen. Zudem erlaubt die Zusammenarbeit mit externen Experten eine flexible Skalierung der Sicherheitsmaßnahmen, die sich an die dynamische Entwicklung der Bedrohungslandschaft anpasst.

In diesem Kontext spielt die Künstliche Intelligenz (KI) eine zunehmend zentrale Rolle. KI-Technologien sind in der Lage, große Datenmengen in Echtzeit zu analysieren, Muster zu erkennen und auch komplexe Angriffsvektoren zu identifizieren, die dem menschlichen Auge verborgen bleiben könnten. Für Mitarbeiter in einem SOC bedeutet der Einsatz von KI eine signifikante Unterstützung. Sie ermöglicht eine effizientere Priorisierung von Sicherheitswarnungen, indem sie Falschpositive reduziert und die Aufmerksamkeit auf tatsächliche Bedrohungen lenkt. Dadurch können Sicherheitsteams schneller und zielgerichteter reagieren und Ressourcen dort einsetzen, wo sie am dringendsten benötigt werden.

Neue Lösungen im Bereich Extended Detection and Response (XDR) integrieren KI, um eine noch umfassendere Analyse und Abwehr von Cyberbedrohungen zu ermöglichen. Beispiele wie CrowdStrike und Darktrace zeigen, wie fortgeschrittene KI-Algorithmen nicht nur Angriffsmuster erkennen, sondern auch in der Lage sind, aus diesen Erkenntnissen zu lernen und ihre Reaktionsmechanismen kontinuierlich zu verbessern.

Dies führt zu einem proaktiveren und adaptiven Sicherheitsmanagement, das in der Lage ist, mit der Evolution von Cyberbedrohungen Schritt zu halten. Die Vorteile der Künstlichen Intelligenz im Bereich der Cybersicherheit sind vielfältig und umfassen eine verbesserte Erkennungsgenauigkeit und eine effizientere Ressourcennutzung. Die Fähigkeit der KI, lernend und adaptiv auf Bedrohungen zu reagieren, bietet ein enormes Potential für die Zukunft der Cyberabwehr.

Es ist davon auszugehen, dass KI-Technologien weiterentwickelt werden, um noch autonomer agieren zu können und Sicherheitsteams durch Vorhersagen zukünftiger Angriffstrends strategische Entscheidungshilfen zu bieten.

KERNTHESEN /

- Im Mittelstand muss ein Bewusstsein für das hohe Risikopotential geschaffen werden
- Es geht nicht um eine völlige Abschottung der Systeme, sondern um eine schlüssige Überlebensstrategie
- Cyber-Sicherheit ist ein dauernder Prozess

Blickt man in die Zukunft, ist klar, dass KI eine immer wichtigere Rolle in der Entwicklung von Cyberabwehrstrategien spielen wird. Die Integration von KI in SOC-Dienstleistungen wird nicht nur die Effizienz und Wirksamkeit der Cybersicherheit erhöhen, sondern auch dazu beitragen, neue Wege im Kampf gegen Cyberkriminalität zu beschreiten. Angesichts der rasanten Entwicklung und Diversifizierung von Cyberbedrohungen wird die kontinuierliche Weiterentwicklung und Anpassung von KI-gestützten Sicherheitslösungen entscheidend sein, um Unternehmen zuverlässig vor zukünftigen Angriffen zu schützen.

Die Implementierung eines eigenen Security Operations Center (SOC) stellt Unternehmen vor eine Vielzahl von Herausforderungen, wobei der Zugang zu qualifiziertem Personal eine der größten Hürden darstellt. Aufgrund der rasanten Entwicklung im Bereich der Cyber-Sicherheit und der stetig wachsenden Bedrohungslandschaft ist die Nachfrage nach erfahrenen Spezialisten, die ein SOC effektiv betreiben können, enorm hoch. Dies führt zu einem hart umkämpften Markt, auf dem qualifizierte Fachkräfte rar und dementsprechend kostspielig sind. Viele Unternehmen, insbesondere kleine und mittelständische, finden sich in einer Situation wieder, in der sie aufgrund begrenzter finanzieller und personeller Ressourcen kaum in der Lage sind, mit großen Konzernen, um diese Spezialisten zu konkurrieren.

Die Spezialisierung, die für die Arbeit in einem SOC erforderlich ist, umfasst ein breites Spektrum an Fähigkeiten, von der tiefgreifenden Kenntnis verschiedener IT-Infrastrukturen über fortgeschrittene Analysefähigkeiten bis hin zu einem umfassenden Verständnis aktueller und potenzieller Cyber-Bedrohungen. Die Ausbildung dieser Experten ist zeitaufwendig und kostspielig, was den Pool verfügbarer Fachkräfte zusätzlich einschränkt. Darüber hinaus erfordert die Dynamik der Cyber-Sicherheitslandschaft eine kontinuierliche Weiterbildung und Anpassung der Fähigkeiten, um mit den sich entwickelnden Bedrohungen Schritt halten zu können. Angesichts dieser Herausforderungen erkennen viele Unternehmen die Vorteile externer SOC-Dienstleistungen. Diese bieten nicht nur Zugang

zu einem Team von Spezialisten, die über das erforderliche Wissen und die Erfahrung verfügen, sondern ermöglichen es den Unternehmen auch, von Skaleneffekten und gemeinsam genutzten Ressourcen zu profitieren. Externe Anbieter können ihre Dienstleistungen über ein breites Spektrum von Kunden hinweg standardisieren und optimieren, was zu Kosteneffizienz und einer höheren Qualität der Sicherheitsüberwachung und -reaktion führt.

Für Unternehmen bedeutet dies, dass sie sich auf ihr Kerngeschäft konzentrieren können, während sie gleichzeitig ein hohes Maß an Cyber-Sicherheit aufrechterhalten, ohne direkt um die begrenzten Ressourcen auf dem Arbeitsmarkt für Cyber-Sicherheitsexperten konkurrieren zu müssen. In einer Zeit, in der Cyber-Bedrohungen immer ausgefeilter werden und die Notwendigkeit einer 24/7-Überwachung der IT-Sicherheit immer wichtiger wird, bietet der Rückgriff auf externe SOC-Dienstleistungen eine praktikable und oft wirtschaftlichere Lösung für das Problem des Fachkräftemangels im Bereich der Cyber-Sicherheit.

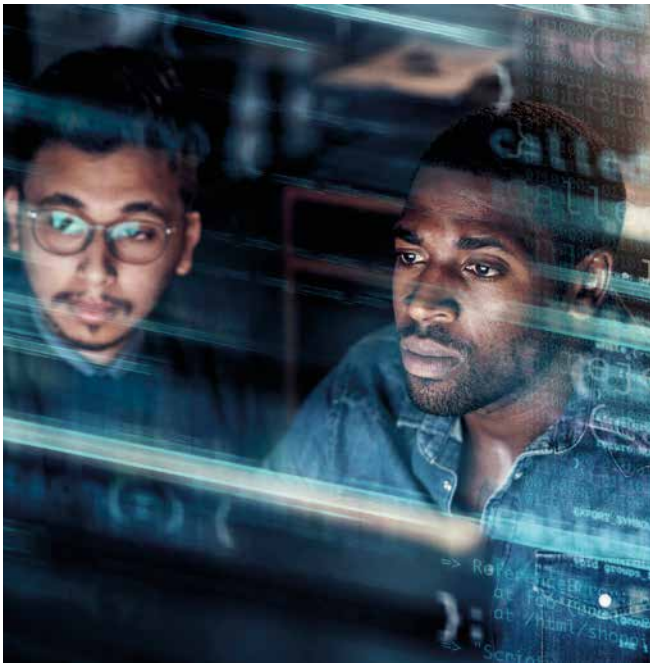
VI. **RESTRISIKO DURCH CYBER-VERSICHERUNGEN ABDECKEN /**

Trotz umfangreicher Sicherheitsmaßnahmen lässt sich ein Restrisiko niemals vollständig eliminieren. Cyber-Versicherungen bieten hier eine zusätzliche Absicherung. Sie decken nicht nur die Kosten für die Wiederherstellung von Daten und Systemen, sondern übernehmen oft auch die Kosten für rechtliche Beratung, Krisenkommunikation und die Haftung gegenüber Dritten. Eine Cyber-Versicherung kann somit einen wichtigen Baustein in der Gesamtstrategie zur Cyber-Sicherheit darstellen.

Die Bedrohung durch Cyber-Angriffe ist für mittelständische Unternehmen real und erfordert eine umfassende Strategie zur Gewährleistung der Cyber-Sicherheit. Durch die Kombination aus präventiven Maßnahmen wie Awareness-Schulungen und der Einrichtung eines SOC, der Implementierung von Backup-Strategien sowie der Absicherung durch Cyber-Versicherungen können Unternehmen ihre Resilienz gegenüber Cyber-Gefahren signifikant erhöhen. Der Schlüssel zum Erfolg liegt dabei in der kontinuierlichen Anpassung der Sicherheitsmaßnahmen an die sich ständig weiterentwickelnde Bedrohungslandschaft.

In der zunehmend digitalisierten Welt von heute, in der die Bedrohungen durch Cyber-Angriffe stetig wachsen, wird die Versicherung von Cyber-Risiken immer wichtiger für Unternehmen aller Größenordnungen. Um das individuelle Risikopotential eines Unternehmens genau zu erfassen, zu analysieren und zu bewerten, ist es ratsam, auf die Expertise von Versicherungsmaklern zurückzugreifen, die über spezialisierte Cyber-Fachabteilungen verfügen. Diese Spezialisten bringen nicht nur ein tiefes Verständnis der komplexen Natur von Cyber-Risiken mit, sondern sind auch darauf geschult, die spezifischen Bedürfnisse und Risiken eines Unternehmens zu identifizieren. Durch eine zielgenaue Ausschreibung des Risikos können sie maßgeschneiderte Versicherungslösungen anbieten, die den individuellen Anforderungen des Unternehmens entsprechen.

Ein entscheidender Aspekt bei der Versicherung von Cyber-Risiken ist die Kosten-Nutzen-Abwägung. Um die Versicherungskosten zu optimieren, empfiehlt es sich für Unternehmen, eine eher hohe Selbstbeteiligung zu wählen. Dies führt dazu, dass kleinere Schadensereignisse vom Unternehmen selbst getragen werden, während die Versicherung für das existenzielle Risiko aufkommt, also für Schäden, die die finanzielle Stabilität des Unternehmens ernsthaft gefährden könnten. Ein solcher Ansatz gewährleistet, dass der Versicherungsschutz dort greift, wo er am meisten benötigt wird, und hält gleichzeitig die Versicherungsprämien in einem wirtschaftlich vertretbaren Rahmen.



Der wesentliche Vorteil einer Cyber-Versicherung liegt jedoch nicht allein im finanziellen Schutz. Versicherer bieten einen Risikotransfer an, der es Unternehmen ermöglicht, einen Teil der Verantwortung und der potenziellen finanziellen Last im Falle eines Cyber-Vorfalls auf den Versicherer zu übertragen.

Dies beinhaltet auch die Abwehr von Schadenersatzansprüchen, die im Zuge von Datenschutzverletzungen und Verstößen gegen die Datenschutz-Grundverordnung (DSGVO)

entstehen können. Angesichts der strengen Regulierungen und hohen Bußgelder, die mit der DSGVO einhergehen, ist dieser Aspekt für Unternehmen von unschätzbarer Bedeutung.

Die größte Bedeutung für die versicherten Unternehmen liegt jedoch im Zugang zu einem umfassenden Netzwerk von Experten, das durch die Versicherer sichergestellt wird. Dieses Netzwerk steht den Unternehmen im Schadensfall rund um die Uhr zur Verfügung. Es umfasst Fachanwälte, die sich auf Cyber-Recht und Datenschutz spezialisiert haben, Forensiker, die die Ursachen und den Umfang eines Cyber-Angriffs untersuchen, Krisenmanager, die bei der Bewältigung des Vorfalls unterstützen, sowie PR-Fachleute, die helfen, den Reputationsschaden zu minimieren. Der Zugang zu diesen Fachleuten kann entscheidend sein, um einen Cyber-Vorfall effektiv zu bewältigen und langfristige Schäden für das Unternehmen zu verhindern.

Versicherer bieten jedoch nur dann Versicherungsschutz an, wenn sich das Unternehmen aktiv und professionell um die technische und organisatorische Sicherheit kümmert. Dies beinhaltet regelmäßige Sicherheitsaudits, die Implementierung von Best Practices in Sachen IT-Sicherheit und Datenschutz sowie die fortlaufende Schulung der Mitarbeiter.

Es handelt sich hierbei um einen kontinuierlichen und regelmäßigen Dialog zwischen Unternehmen, Versicherungsmakler und Versicherer, da sich das Risikofeld dynamisch verändert und fortwährend neuen Bedrohungen ausgesetzt ist.

Die Cyber-Versicherung spielt somit eine zentrale Rolle in der modernen Risikomanagementstrategie eines Unternehmens. Sie bietet nicht nur finanziellen Schutz und unterstützt bei der Compliance mit Datenschutzgesetzen, sondern gewährt auch Zugang zu einem unverzichtbaren Netzwerk von Experten, die im Notfall unterstützen können. Dieser ganzheitliche Ansatz macht die Cyber-Versicherung zu einem unverzichtbaren Instrument für Unternehmen, um sich in der digitalen Ära effektiv gegen die wachsenden Cyber-Risiken zu wappnen.

ZUSAMMENFASSUNG /

- Ein Großteil der Cyber-Risiken ist beherrschbar
- Im Risiko-Management der Unternehmen müssen Cyber-Risiken eine wesentliche Rolle spielen und die Geschäftsführung muss eng eingebunden sein
- Existenzielle Risiken können an Versicherer transferiert werden

ÜBER ARTUS /

Die ARTUS GRUPPE gehört zu den Top-Versicherungsmaklern in Deutschland und der Schweiz mit mehr als 500 Mitarbeitenden an 16 Standorten. Sie erstellt Absicherungskonzepte gegen Cybergefahren für Unternehmen des Mittelstands und der mittelständischen Industrie gegen eine Vielzahl von Risiken wie Betrugsschäden, Schadenersatzansprüchen, Vertragsstrafen, Betriebsunterbrechungen und anderer Kosten, die mit Hackerangriffen und Cyber-Gefahren zusammenhängen.

ÜBER DEN AUTOR /

Marcus Unger ist Leiter des Competence Centers Cyber Nord und verantwortet die Bereiche Risikoerfassung, Risikobewertung und Cyber-Incident-Management. Er berät seit über 20 Jahren erfolgreich Kundenunternehmen hinsichtlich Ihrer Cyberabdeckung und Ihrer Cybersicherheit.

DAS ARTUS CYBER TEAM BERÄT SIE GERNE /

/ MARCUS UNGER /

Head of Competence Center Cyber Nord, Cyber-Experte
ARTUS Osnabrück

marcus.unger@artus-gruppe.com

/ MARKUS WAGNER /

Head of Comeptence Center Cyber Süd, Leiter Sachversicherung
ARTUS Friedrich Ganz

markus.wagner@artus-gruppe.com

/ FELIX RÖDER /

Cyber-Experte,
Stellvertretender Leiter Analyse
ARTUS Friedrich Ganz

felix.roeder@artus-gruppe.com

ARTUS GRUPPE /

GEMEINSAM EINFACH MACHEN

www.artus-gruppe.com