JULI 2025

IHR WEG ZUR OPTIMALEN CYBER-VERSICHERUNG UND ROBUSTEN IT-SICHERHEIT

PLAYBOOK: CYBER-RESILIENZ STÄRKEN

Dorner Systems

Playbook: Cyber-Resilienz stärken

IHR WEG ZUR OPTIMALEN CYBER-VERSICHERUNG UND ROBUSTEN IT-SICHERHEIT

Sehr geehrte Unternehmerin, sehr geehrter Unternehmer,

in der heutigen digitalen Welt ist Cybersicherheit keine Option mehr, sondern eine absolute Notwendigkeit. Die Bedrohungslandschaft entwickelt sich rasant, und Unternehmen jeder Größe sind potenzielle Ziele von Cyberangriffen. Die Folgen eines erfolgreichen Angriffs – Datenverlust, Betriebsunterbrechungen, Reputationsschäden und hohe Kosten – können existenzbedrohend sein. Eine Cyber-Security-Versicherung bietet hier einen wichtigen Schutzschirm, indem sie finanzielle Risiken abfedert. Doch der Abschluss einer solchen Versicherung ist komplex und erfordert, dass Ihr Unternehmen bestimmte Sicherheitsstandards erfüllt.

Dieses Playbook dient Ihnen als umfassender Leitfaden. Es erklärt nicht nur, warum eine Cyber-Versicherung unerlässlich ist, sondern auch, welche Schritte Sie unternehmen müssen, um Ihr Unternehmen optimal auf einen solchen Schutz vorzubereiten. Wir beleuchten die rechtlichen und unternehmerischen Gründe für Investitionen in Cybersicherheit, stellen Ihnen die besten Versicherungsanbieter vor und geben Ihnen detaillierte Anleitungen und Checklisten an die Hand, um Ihre IT-Infrastruktur zu prüfen und zu optimieren. Darüber hinaus zeigen wir Ihnen, wie Sie durch proaktive Maßnahmen nicht nur eine günstigere Versicherung erhalten, sondern auch die allgemeine Stabilität und Leistungsfähigkeit Ihres Netzwerks nachhaltig verbessern. Denken Sie daran: Ein starkes Fundament an Cybersicherheit ist die beste Voraussetzung für den Erfolg Ihres Unternehmens und minimiert Risiken im Ernstfall.

1. WARUM CYBERSICHERHEIT UND EINE CYBER-VERSICHERUNG UNVERZICHTBAR SIND

Ein Cyberangriff ist für viele Unternehmen ein Damoklesschwert. Die Auswirkungen gehen weit über den rein finanziellen Schaden hinaus. Stellen Sie sich vor, Ihr Betrieb steht still, weil die Systeme verschlüsselt sind, Kundendaten geleakt wurden oder Ihre gesamte Kommunikation lahmgelegt ist. Das Vertrauen Ihrer Kunden schwindet, rechtliche Konsequenzen drohen, und die Wiederherstellung der Systeme kann Wochen oder Monate dauern. Selbst kleine Unternehmen mit nur wenigen Mitarbeitern sind attraktive Ziele, da sie oft über weniger robuste Sicherheitsvorkehrungen verfügen. Die Kosten für die Behebung eines Cyberangriffs können für KMU existenzbedrohend sein und im schlimmsten Fall zur Insolvenz führen. Eine Cyber-Security-Versicherung bietet hier einen finanziellen Schutz und unterstützt Sie bei der Bewältigung der Krisensituation, doch sie ist nur ein Teil der Lösung. Die eigentliche Stärke liegt in einer proaktiven und umfassenden IT-Sicherheitsstrategie, die Angriffe von vornherein abwehrt und Ihr Unternehmen resilient macht.

Checkliste: Risikobewertung und Notwendigkeit der Cyber-Versicherung

- Ist Ihnen bewusst, welche sensiblen Daten in Ihrem Unternehmen gespeichert sind (Kunden-, Mitarbeiterdaten, Geschäftsgeheimnisse)?
- Kennen Sie die potenziellen Kosten eines Cyberangriffs (Betriebsausfall, Datenwiederherstellung, rechtliche Konsequenzen)?
- Haben Sie bereits einen Notfallplan für den Fall eines Cyberangriffs?!
- Sind Ihre Mitarbeiter regelmäßig zum Thema Cybersicherheit geschult?
- Verstehen Sie die rechtlichen Verpflichtungen (z.B. DSGVO) bei einem Datenleck?
- Sind Sie sich bewusst, dass auch kleine Unternehmen attraktive Ziele für Cyberkriminelle sind?
- Haben Sie die finanziellen Auswirkungen eines längeren Betriebsausfalls bedacht?
- Wissen Sie, welche Reputationsschäden ein Cyberangriff verursachen kann?

2. DIE WAHL DER RICHTIGEN CYBER-VERSICHERUNG: EMPFEHLUNGEN FÜR UNTERNEHMEN (20-100 MITARBEITER)

Die Auswahl der passenden Cyber-Versicherung ist entscheidend und hängt stark von den individuellen Bedürfnissen und Risikoprofilen Ihres Unternehmens ab. Es gibt eine Vielzahl von Anbietern auf dem Markt, die unterschiedliche Deckungsumfänge und Leistungen anbieten. Für Unternehmen mit 20-100 Mitarbeitern sind vor allem Versicherer interessant, die sich auf KMU spezialisiert haben und modular aufgebaute Policen anbieten, um eine bedarfsgerechte Absicherung zu gewährleisten. Achten Sie auf transparente Bedingungen, schnelle Schadensregulierung und Zusatzleistungen wie präventive Beratung oder Zugang zu Expertennetzwerken. Die Prämienhöhe wird maßgeblich von Ihrem Sicherheitsniveau beeinflusst, daher lohnt sich jede Investition in IT-Sicherheit doppelt. Beachten Sie, dass eine jährliche Zahlweise oft günstiger ist als eine monatliche, aber prüfen Sie die Liquidität Ihres Unternehmens, um die beste Option zu wählen.

Top-3-Vorschläge für Cyber-Versicherungen (Beispielhaft und ohne Gewähr, da sich der Markt ständig ändert)

Hiscox: Oft gelobt für maßgeschneiderte Lösungen für KMU und eine gute Betreuung im Schadensfall. Bietet modulare Deckungsoptionen, die sich an die spezifischen Bedürfnisse anpassen lassen**.**

- ***Besondere Merkmale:*** Fokus auf schnellen Incident Response, flexible Deckung, auch für Betriebsunterbrechungen.
- ***Ideal für:*** Unternehmen, die Wert auf einen umfassenden Schutz und schnelle Hilfe im Ernstfall legen.

Allianz: Als großer und etablierter Versicherer bietet die Allianz robuste Cyber-Policen mit breitem Leistungsspektrum. Hier profitieren Sie von der Erfahrung und Finanzkraft eines Global Players.

- ***Besondere Merkmale:*** Solide Absicherung, oft inklusive Forensik-Kosten, Reputationsschutz und Rechtsberatung.
- ***Ideal für:*** Unternehmen, die einen zuverlässigen und finanziell starken Partner suchen.

ERGO: Die ERGO bietet ebenfalls spezielle Cyber-Versicherungen für mittelständische Unternehmen an. Sie zeichnet sich oft durch ein gutes Preis-Leistungs-Verhältnis und kundenfreundliche Konditionen aus.

- ***Besondere Merkmale:*** Häufig inklusive Kosten für PR-Beratung nach einem Vorfall und Unterstützung bei der Wiederherstellung von Daten.
- ***Ideal für:*** Unternehmen, die einen ausgewogenen Mix aus Leistung und Kosten suchen.

Checkliste: Auswahlkriterien für die Cyber-Versicherung

- Welche Schadensarten sind abgedeckt (Datenverlust, Betriebsunterbrechung, Reputationsschäden, Lösegeldforderungen)?
- Wie hoch sind die Deckungssummen für die einzelnen Bereiche?
- Welche Selbstbeteiligung ist vorgesehen?
- Welche Ausschlüsse gibt es (z.B. grobe Fahrlässigkeit, vorhandene, bekannte Schwachstellen)?
- Bietet die Versicherung Unterstützung bei der Incident Response (Forensiker, Rechtsberatung, PR)?
- Werden präventive Maßnahmen des Unternehmens berücksichtigt (günstigere Prämien)?
- Wie ist der Ruf des Versicherers im Bereich Cyber-Schadensregulierung?
- Gibt es Zusatzleistungen wie Cyber-Security-Trainings für Mitarbeiter?

3. KERNPUNKTE EINER CYBERSECURITY-VERSICHERUNG: WAS SIE BEACHTEN MÜSSEN

Der Abschluss einer Cyber-Security-Versicherung ist kein Selbstläufer. Versicherer verlangen in der Regel eine detaillierte Prüfung Ihrer IT-Sicherheitsmaßnahmen, um das Risiko korrekt einschätzen zu können. Dazu gehören Fragen zu Ihrer Infrastruktur, Ihren Richtlinien und Ihren Notfallplänen. Es ist von größter Bedeutung, dass Sie diese Fragen ehrlich und umfassend beantworten. Eine lückenhafte oder falsche Angabe kann im Schadensfall zur Ablehnung der Leistung führen. Die Anforderungen reichen von grundlegenden Sicherheitsmaßnahmen wie Firewalls und Virenschutz bis hin zu

komplexeren Themen wie Netzwerksegmentierung, regelmäßigen Backups und Incident-Response-Plänen. Je besser Ihr Unternehmen in diesen Bereichen aufgestellt ist, desto geringer ist nicht nur das Risiko eines Angriffs, sondern auch die Prämie für Ihre Versicherung. Eine transparente Dokumentation aller Sicherheitsmaßnahmen ist dabei unerlässlich.

Checkliste: Wichtige Punkte für die Cyber-Versicherung

Netzwerksicherheit:

- Verwenden Sie eine Firewall mit aktuellen Filterregeln für ein- und ausgehenden Traffic?
- Ist Ihr Netzwerk segmentiert (Trennung von produktiven Systemen, Gastnetzwerken, IoT-Geräten)?
- Werden VPN-Verbindungen für externen Zugriff sicher genutzt und regelmäßig überprüft?
- Sind Drucker und andere Netzwerkgeräte über ein Management-Interface abgesichert?
- Werden Smart-Home-Geräte oder Maschinen im Netzwerk separat abgesichert und dokumentiert?

Endpunkt-Sicherheit:

- Sind alle Endgeräte (PCs, Laptops, Server) mit einem aktuellen Antivirenprogramm ausgestattet?
- Wird ein Endpoint Detection and Response (EDR) oder vergleichbares System eingesetzt, das erweiterte Sicherheitsfunktionen bietet?
- Sind Betriebssysteme (z.B. Windows 10/11) und Anwendungen auf dem neuesten Stand (Patch Management)?
- Gibt es eine Richtlinie für die Nutzung von Wechselmedien (USB-Sticks)?

Daten- und Zugriffssicherheit:

- Werden regelmäßige Backups aller wichtigen Daten erstellt und außerhalb des primären Netzwerks gesichert (z.B. 3-2-1-Regel)?
- Werden Backups regelmäßig auf ihre Wiederherstellbarkeit getestet?
- Gibt es eine Passwortrichtlinie (Komplexität, regelmäßige Änderung, Multi-Faktor-Authentifizierung)?
- Sind Zugriffsrechte auf Basis des "Need-to-know"-Prinzips vergeben und werden regelmäßig überprüft?
- Wird eine E-Mail-Verschlüsselung und/oder Signierung eingesetzt (z.B. S/MIME, PGP)?

Notfallmanagement und Dokumentation:

- Existiert ein Notfallplan für den Cyber-Angriff (Incident Response Plan)?
- Sind Ansprechpartner und Notrufnummern (intern/extern) klar definiert und kommuniziert?
- Gibt es eine aktuelle und detaillierte Netzwerkdokumentation (Topologie, Geräte, Software-Assets)?
- Wird die Softwareinventarisierung und -priorisierung regelmäßig durchgeführt?
- Existieren Sicherheitsrichtlinien für Mitarbeiter (z.B. zur Nutzung von E-Mails, Internet, mobilen Geräten)?

Mitarbeiter und Homeoffice/Mobile Arbeitsplätze:

- Werden Mitarbeiter regelmäßig in Cybersicherheit geschult (Phishing, Social Engineering)?
- Gibt es klare Richtlinien für die Nutzung von mobilen Arbeitsplätzen und Homeoffice?
- Wird beim Homeoffice-Arbeitsplatz die elektrische Prüfung und ergonomische Ausstattung gemäß den rechtlichen Vorgaben durchgeführt?
- Sind die vom Arbeitgeber bereitgestellten Hardware-Komponenten (Tische, Stühle, Monitore, Computer) für Homeoffice-Arbeitsplätze dokumentiert und geprüft?

4. RECHTLICHE UND UNTERNEHMERISCHE GRÜNDE FÜR PROAKTIVE CYBERSICHERHEIT

Die Motivation für eine umfassende Cybersicherheitsstrategie geht weit über die Anforderungen einer Versicherung hinaus. Rechtlich sind Unternehmen in Deutschland durch Gesetze wie die DSGVO und das IT-Sicherheitsgesetz 2.0 dazu verpflichtet, angemessene technische und organisatorische Maßnahmen zum Schutz von Daten und Systemen zu ergreifen. Ein Verstoß kann hohe Bußgelder nach sich ziehen und die Geschäftsführung persönlich in die Pflicht nehmen. Unternehmerisch gesehen ist eine robuste IT-Sicherheit der Grundstein für einen reibungslosen Betriebsablauf und die Minimierung von Risiken. Ein gesichertes Netzwerk bedeutet weniger Ausfallzeiten, höhere Produktivität und einen besseren Schutz Ihrer wertvollen Geschäftsdaten. Zudem stärkt es das Vertrauen Ihrer Kunden und Partner, was wiederum Ihre Marktposition festigt. Sehen Sie Cybersicherheit nicht als Kostenfaktor, sondern als strategische Investition in die Zukunft und Stabilität Ihres Unternehmens.

Checkliste: Rechtliche und unternehmerische Aspekte der Cybersicherheit

- Sind Sie über die aktuellen Datenschutzbestimmungen (z.B. DSGVO) informiert?
- Kennen Sie Ihre Meldepflichten bei Datenpannen an Aufsichtsbehörden?
- Haben Sie einen Datenschutzbeauftragten benannt (falls erforderlich)?
- Wie beeinflusst die IT-Sicherheit die Kontinuität Ihrer Geschäftsprozesse?
- Welchen Wettbewerbsvorteil können Sie durch ein hohes Sicherheitsniveau erzielen?
- Wie bewerten Ihre Kunden und Partner Ihre IT-Sicherheit?
- Welche Auswirkungen hätte ein längerer Systemausfall auf Ihre Lieferketten?
- Sind Sie sich der persönlichen Haftung als Geschäftsführer bei unzureichenden Sicherheitsmaßnahmen bewusst?

5. IHR VORTEIL: EINE IT-FLATRATE UND MANAGED SERVICES FÜR MEHR SICHERHEIT UND EFFIZIENZ

Ein großes Missverständnis ist, dass IT-Sicherheit nur durch interne Ressourcen gewährleistet werden kann. Oftmals ist dies jedoch nicht praktikabel oder wirtschaftlich, insbesondere für KMU. Eine IT-Flatrate oder die Nutzung von Managed Services durch einen externen Dienstleister bietet hier erhebliche Vorteile. Zum einen erhalten Sie Zugang zu einem Team von Spezialisten, die über umfassendes Wissen und aktuelle Informationen zu Bedrohungen und Schutzmaßnahmen verfügen. Dies gewährleistet eine hohe Expertise und schnelle Reaktionszeiten. Zum anderen profitieren Sie von transparenten, planbaren Kosten, da ein monatlicher Festpreis vereinbart wird, anstatt teure Einzelabrechnungen nach Minutentaktung.

Ein externer Dienstleister kümmert sich um essenzielle Aufgaben wie Monitoring, Patch Management, Remote Support und die Pflege Ihrer Netzwerkdokumentation. Dadurch werden Ihre internen Mitarbeiter entlastet, und Sie können sich auf Ihr Kerngeschäft konzentrieren. Die kontinuierliche Überwachung Ihrer Systeme hilft, Probleme frühzeitig zu erkennen und zu beheben, bevor sie zu schwerwiegenden Ausfällen führen.
Zudem stellt ein externer Dienstleister sicher, dass Ihre Systeme stets auf dem neuesten Stand sind und potenzielle Sicherheitslücken geschlossen werden. Dies ist nicht nur gut für die interne Effizienz, sondern auch ein entscheidender Nachweis für Ihre Cyber-Versicherung, der Ihnen zu günstigeren Prämien verhelfen kann. Ein einzelner IT-Mitarbeiter oder eine "One-Man-Show" birgt hingegen erhebliche Risiken: Bei Krankheit, Urlaub oder einem Unfall ist die Expertise und Dokumentation nicht verfügbar, was Ihr Unternehmen im Ernstfall handlungsunfähig macht. Ein Team externer Experten bietet hier die notwendige Ausfallsicherheit und Expertise.

Checkliste: Vorteile externer IT-Dienstleister und Managed Services

Finanzielle Vorteile:

- Reduzierung unerwarteter Kosten durch eine IT-Flatrate und planbare monatliche Ausgaben.
- Potenziell günstigere Prämien für die Cyber-Versicherung durch professionelles Management.
- Kostenersparnis im Vergleich zu einer vollwertigen internen IT-Abteilung.

Sicherheitsvorteile:

- Kontinuierliches Monitoring und frühzeitige Erkennung von Bedrohungen.
- Professionelles Patch Management für Betriebssysteme, Anwendungen und Hardware (z.B. Firewall, Router).
- Zugang zu Expertenwissen und aktuellen Informationen über Cyber-Bedrohungen.
- Sicherstellung der Netzwerksegmentierung und Absicherung komplexer Geräte (NAS, Drucker, IoT).
- Regelmäßige Backups und Prüfung der Wiederherstellbarkeit.

Operative Vorteile:

- Entlastung der internen Mitarbeiter und Fokus auf das Kerngeschäft.
- Schnelle Reaktionszeiten bei Supportanfragen (IT-Flatrate vs. minutengenau).
- Professionelle und stets aktuelle Netzwerkdokumentation.
- Zugriff auf Software- und Hardware-Assets-Listen über Monitoring-Systeme.
- Sicherstellung, dass veraltete Systeme (Windows XP, alte Server, alte Firewalls) aus dem Netzwerk entfernt oder adäquat geschützt werden.
- Vermeidung von Abhängigkeiten von einer "One-Man-Show" und Sicherstellung der Verfügbarkeit von IT-Know-how.

6. SO OPTIMIEREN SIE IHRE IT-INFRASTRUKTUR FÜR DIE CYBER-VERSICHERUNG UND DEN GESCHÄFTSBETRIEB

Die Anforderungen der Cyber-Versicherer spiegeln bewährte Praktiken der IT-Sicherheit wider. Indem Sie diese Maßnahmen implementieren, schützen Sie nicht nur Ihr Unternehmen, sondern erhöhen auch Ihre Chancen auf eine günstigere Prämie. Beginnen Sie mit einer detaillierten Inventarisierung Ihrer IT-Assets: Welche Hardware und Software wird eingesetzt? Wo befinden sich sensible Daten? Anschließend sollten Sie Ihre Sicherheitsrichtlinien überprüfen und gegebenenfalls anpassen. Hierzu gehören klare Regeln für Passwörter, E-Mail-Nutzung, den Umgang mit mobilen Geräten und die Internetnutzung. Ein besonderes Augenmerk sollte auf der Netzwerksegmentierung liegen, um eine Ausbreitung von Schadsoftware im Falle eines Angriffs zu verhindern.

Implementieren Sie moderne Firewalls, die auch Ransomware und Hackerangriffe abwehren können, und stellen Sie sicher, dass Ihr Antivirenschutz den eingehenden Traffic auf Viren und Schadcode prüft. Denken Sie auch an die Absicherung von Druckern und NAS-Systemen über deren Management-Interfaces.

Checkliste: Optimierung der IT-Infrastruktur

Hardware-Inventarisierung:

- Erfassen Sie alle Computer, Server, Notebooks, Drucker, Router, NAS-Systeme und andere netzwerkfähige Geräte.
- Überprüfen Sie das Alter der Hardware: Sind Firewalls und Server aktuell genug, um moderne Sicherheitsstandards zu erfüllen?
- Dokumentieren Sie die Funktionen jedes Geräts (z.B. Router mit Firewall-Funktionen, Antiviren-Schutz für eingehenden Traffic).

Software-Inventarisierung und Priorisierung:

- Erstellen Sie eine Liste aller installierten Software (Betriebssysteme, Anwendungen, Spezialsoftware).
- Identifizieren Sie kritische Software für Ihren Geschäftsbetrieb.
- Stellen Sie sicher, dass alle Betriebssysteme aktuell sind (Windows 10/11). Windows XP und ältere Server sollten aus dem Netzwerk entfernt werden.

Netzwerk- und Gerätesicherheit:

- Implementieren Sie eine Next-Generation-Firewall, die Ransomware und Hacker-Netze blockieren kann und eingehenden Traffic auf Viren und Schadcode prüft.
- Stellen Sie sicher, dass Filterregeln für den Datenverkehr von innen nach außen und außen nach innen präzise definiert sind.
- Führen Sie eine Netzwerksegmentierung durch, um kritische Bereiche zu isolieren.
- Sichern Sie Drucker, NAS-Systeme und Router über ihre Management-Interfaces ab und ändern Sie Standardpasswörter.
- Überprüfen Sie die Konfiguration von VPN-Verbindungen auf deren Sicherheit.

Datensicherung und Notfallplanung:

- Implementieren Sie eine robuste Backup-Strategie (z.B. 3-2-1-Regel).
- Testen Sie die Wiederherstellbarkeit Ihrer Backups regelmäßig.
- Erstellen Sie einen umfassenden Notfallplan für den Cyber-Angriff, der Rollen, Verantwortlichkeiten und Wiederherstellungsschritte klar definiert.
- Definieren Sie Notrufnummern und Ansprechpartner für den Ernstfall.

7. HOMEOFFICE VS. MOBILER ARBEITSPLATZ: RECHTLICHE UND TECHNISCHE UNTERSCHIEDE

Die Arbeitswelt hat sich verändert, und flexible Arbeitsmodelle wie Homeoffice und mobile Arbeit sind Standard geworden. Doch aus rechtlicher und technischer Sicht gibt es wesentliche Unterschiede, die auch für die Cyber-Versicherung relevant sind. Ein Homeoffice-Arbeitsplatz ist ein fester Arbeitsplatz in der Privatwohnung des Mitarbeiters. Hier gelten strenge Regeln: Der Arbeitgeber ist für die Bereitstellung der gesamten notwendigen Hardware (Tische, Stühle, Monitore, Computer) verantwortlich und muss jährlich eine Elektro-Prüfung sowie eine ergonomische Bewertung des Arbeitsplatzes vor Ort durchführen lassen. Technisch muss der Homeoffice-Arbeitsplatz so abgesichert sein wie ein Büroarbeitsplatz, inklusive sicherer VPN-Verbindungen und aktueller Sicherheitssoftware.

Ein mobiler Arbeitsplatz hingegen ist flexibler. Der Mitarbeiter arbeitet von wechselnden Orten aus, und der Arbeitgeber stellt lediglich die benötigten mobilen Geräte (z.B. Laptop) zur Verfügung. Die Verantwortung für die Ausstattung des Arbeitsplatzes liegt hier nicht beim Arbeitgeber. Technisch müssen die mobilen Geräte besonders gut geschützt sein, da sie oft in unsicheren Netzwerken (z.B. öffentliches WLAN) verwendet werden. Dies erfordert starke Verschlüsselung, Multi-Faktor-Authentifizierung und zuverlässige Sicherheitssoftware. Die Cyber-Versicherung wird diese Unterschiede genau prüfen, da sie unterschiedliche Risikoprofile darstellen. Eine klare Dokumentation und Einhaltung der jeweiligen Vorgaben ist daher essenziell.

Checkliste: Homeoffice und Mobile Arbeitsplätze

Homeoffice-Arbeitsplatz:

- Ist die Hardware (Tische, Stühle, Monitore, Computer) vom Arbeitgeber bereitgestellt?
- Wird eine jährliche Elektro-Prüfung der Geräte vor Ort durchgeführt?
- Wird die Ergonomie des Arbeitsplatzes regelmäßig geprüft?
- Sind sichere VPN-Verbindungen für den Zugriff auf Unternehmensressourcen eingerichtet?
- Gibt es eine klare Datenschutzrichtlinie für das Homeoffice?

Mobiler Arbeitsplatz:

- Werden nur die mobilen Geräte (Laptops, Tablets) vom Arbeitgeber bereitgestellt?
- Ist auf den Geräten eine starke Verschlüsselung aktiviert?
- Wird Multi-Faktor-Authentifizierung für alle Zugriffe genutzt?
- Ist ein aktueller Virenschutz und eine Firewall auf den mobilen Geräten vorhanden?
- Werden Mitarbeiter zum sicheren Umgang mit öffentlichen WLANs geschult?

8. WAS PASSIERT, WENN SIE GEHACKT WERDEN? DIE NOTWENDIGKEIT DER VORSORGE

Die Vorstellung, gehackt zu werden, ist beängstigend, doch sie ist eine reale Bedrohung für jedes Unternehmen. Und die Auswirkungen können weitaus gravierender sein, als viele glauben. Ein Hack bedeutet oft nicht nur den Verlust von Daten oder eine Betriebsunterbrechung, sondern kann die gesamte Existenz Ihres Unternehmens gefährden. Auch kleine Firmen sind nicht immun; im Gegenteil, sie sind oft leichtere Ziele für Cyberkriminelle, die sich "einen Spaß machen" oder geringe Lösegeldforderungen stellen, die aber trotzdem das Unternehmen an den Rand des Ruins treiben können.

Fälle wie die, in denen Unternehmen nach einem Hackerangriff schließen mussten oder enorme Geldsummen verloren haben, sind keine Seltenheit. Lange Ausfallzeiten, der Verlust von Kundendaten, Reputationsschäden und hohe Kosten für die Wiederherstellung können zu einem Teufelskreis führen.

Eine Cyber-Security-Versicherung und die Investition in einen externen IT-Dienstleister sind im Vergleich zu diesen potenziellen Verlusten minimal. Sie dienen als essenzielle Schutzschilde, die nicht nur finanzielle Schäden abfedern, sondern auch die Wiederherstellung beschleunigen und das Risiko insgesamt minimieren. Zeigen Sie Ihren Kunden, dass Sie Cybersicherheit ernst nehmen – es ist ein Vertrauensfaktor, der Ihr Unternehmen stärkt und zukunftssicher macht.

Checkliste: Folgen eines Cyberangriffs und präventive Maßnahmen

Mögliche Folgen eines Hacks:

- Betriebsunterbrechung und damit verbundener Umsatzverlust.
- Datenverlust oder -verschlüsselung (Ransomware).
- Reputationsschäden und Vertrauensverlust bei Kunden.
- Finanzielle Verluste durch Lösegeldforderungen oder Wiederherstellungskosten.
- Rechtliche Konsequenzen und Bußgelder (z.B. DSGVO-Verstöße).
- Existenzbedrohung des Unternehmens.

Vorteile von Cyber-Versicherung und externem IT-Dienstleister:

- Finanzieller Schutz vor den Kosten eines Cyberangriffs.
- Schnellere Wiederherstellung durch professionelle Unterstützung.
- Minimierung des Risikos durch präventive Maßnahmen.
- Zugang zu Expertise im Notfall.
- Nachweis der Sorgfaltspflicht gegenüber Kunden und Partnern.
- Kontinuierliche Verbesserung der IT-Sicherheit durch externes Monitoring und Patching.

9. CHECKLISTEN FÜR DIE SICHERHEIT IHRER GERÄTE

Eine umfassende Gerätesicherheit ist der Grundpfeiler Ihrer gesamten IT-Sicherheitsstrategie. Jedes einzelne Gerät im Netzwerk, vom PC bis zum IoT-Sensor, stellt ein potenzielles Einfallstor für Angreifer dar. Daher ist es unerlässlich, jeden Endpunkt detailliert zu prüfen und abzusichern. Diese Checklisten sollen Ihnen dabei helfen, systematisch vorzugehen und sicherzustellen, dass keine Schwachstellen übersehen werden. Beachten Sie, dass diese Prüfungen regelmäßig durchgeführt und die Ergebnisse dokumentiert werden sollten. Bei komplexen Systemen oder Unsicherheiten ist es ratsam, einen erfahrenen IT-Dienstleister hinzuzuziehen. Denken Sie daran: Ein einziges unsicheres Gerät kann die gesamte Netzwerksicherheit kompromittieren.

Checkliste für PCs und Laptops

Betriebssystem und Software:

- Ist das Betriebssystem (Windows 10/11) aktuell und sind alle Sicherheitsupdates installiert?
- Ist eine Antiviren-Software installiert und aktuell (Signaturen)?
- Wird eine Endpoint Detection and Response (EDR) Lösung eingesetzt?
- Sind alle Anwendungen aktuell und gepatcht?
- Werden unbenötigte Programme deinstalliert?

Sicherheitseinstellungen:

- Ist die lokale Firewall aktiviert und korrekt konfiguriert?
- Sind alle Daten auf dem Laufwerk verschlüsselt (z.B. BitLocker)?
- Sind Passwörter komplex (mind. 12 Zeichen, Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen) und werden regelmäßig geändert?
- Ist Multi-Faktor-Authentifizierung für wichtige Konten aktiviert?
- Sind Administratorrechte auf das Notwendigste beschränkt?
- Werden USB-Sticks und andere Wechselmedien nur von vertrauenswürdigen Quellen genutzt?

Nutzungsverhalten:

- Werden E-Mails und Links von unbekannten Absendern mit Vorsicht behandelt (Phishing-Awareness)?
- Werden nur vertrauenswürdige WLAN-Netzwerke genutzt, insbesondere bei mobilen Geräten (VPN)?
- Checkliste für Server (Windows und Linux)

Betriebssystem und Dienste:

- Ist das Server-Betriebssystem aktuell und sind alle Sicherheitsupdates installiert?
- Werden nur notwendige Dienste ausgeführt (Deaktivierung ungenutzter Dienste)?
- Sind Standard-Ports geändert oder gesichert?
- Wird eine Server-Firewall eingesetzt und sind die Regeln restriktiv konfiguriert?

Zugriff und Berechtigungen:

- Werden starke Passwörter und Multi-Faktor-Authentifizierung für Administratorzugänge verwendet?
- Sind Zugriffsrechte auf Basis des "Least Privilege"-Prinzips vergeben?
- Gibt es eine zentrale Benutzerverwaltung (z.B. Active Directory) mit klaren Richtlinien?
- Werden Login-Versuche protokolliert und überwacht?

Datensicherung und Wiederherstellung:

- Werden regelmäßige Backups aller Serverdaten erstellt?
- Werden Backups regelmäßig auf ihre Wiederherstellbarkeit getestet?
- Sind Backups getrennt vom Netzwerk gespeichert (Offline-Backups)?

Überwachung und Protokollierung:

- Wird die Server-Aktivität kontinuierlich überwacht (Monitoring-System)?
- Werden Protokolldateien regelmäßig analysiert und archiviert?
- Checkliste für Router und Firewalls

Basiskonfiguration:

- Wurde das Standard-Administratorpasswort geändert?
- Ist die Firmware aktuell?
- Sind nicht benötigte Dienste deaktiviert (z.B. UPnP)?

Firewall-Regeln:

- Sind die Filterregeln restriktiv und nur notwendige Ports geöffnet?
- Werden eingehende Verbindungen von unbekannten Quellen blockiert?
- Werden ausgehende Verbindungen überwacht und unsichere Verbindungen blockiert?
- Ist ein Intrusion Detection/Prevention System (IDS/IPS) aktiviert und konfiguriert?
- Ist ein Antiviren-/Malware-Schutz für den Netzwerkverkehr integriert?

Fernzugriff:

- Ist der Fernzugriff nur über sichere VPN-Verbindungen möglich?
- Wird Multi-Faktor-Authentifizierung für VPN-Zugriffe eingesetzt?
- Checkliste für Drucker, NAS-Systeme und IoT/Smart-Home-Geräte im Netzwerk

Zugangssicherheit:

- Wurden Standard-Passwörter für die Management-Interfaces geändert?
- Sind die Management-Interfaces nur aus dem internen Netzwerk erreichbar und nicht aus dem Internet?
- Sind Zugriffsrechte auf diese Geräte eingeschränkt?

Netzwerksegmentierung:

- Sind diese Geräte in einem separaten Netzwerksegment (z.B. IoT-Netzwerk, Drucker-VLAN) isoliert?
- Sind nur die notwendigen Kommunikationswege zu diesen Geräten erlaubt?

Nimm Kontakt auf

Buche ein kostenloses Beratungsgespräch mit Lars Dorner

Kläre deine offene Fragen, bespreche deine Vorgehensweise und stelle sie auf den Prüfstand.

Erhalte zusätzliche Informationen passend zu deinem Unternehmen.

>Klick<: **Termin buchen!**

E-Mail: **kontakt@dorner-systems.de**

Web: **www.dorner-systems.de**

Tel.: **+49 234 97843530**