Ihr Unternehmen im Zeitalter der Cyberkriminalität

7 Strategien für eine proaktive Business Security

7 Strategien für eine proaktive Business Security

Ihr Unternehmen im Zeitalter der Cyberkriminalität

01

Am Thema Business Security kommen Sie nicht vorbei

Cyberkriminalität bedroht die Sicherheit der Deutschen so stark wie nie zuvor

„Cloud-Anbieter geht nach Hackerangriff pleite", „Neuausrichtung nach Hackerangriff", „Tausende Firmen weltweit lahmgelegt", „Hacker greifen Internetseiten der Polizei an", „BSI: Hunderte deutsche Unternehmen von Hackerangriff betroffen", „Angriffswelle auf deutsche Unternehmen".

So oder so ähnlich tönt es mittlerweile täglich aus diversen Nachrichtenkanälen. Die Zeiten, in denen Cybersicherheit ein Randthema für IT-Abteilungen war, sind längst vorbei. Heute steht sie im Zentrum des strategischen Managements eines jeden Unternehmens – oder sollte es zumindest.

Warum können wir das Thema nicht ignorieren?

Die Abhängigkeit von IT-Systemen ist immens und wächst mit jeder digitalen Innovation. Vom Kundenmanagement bis hin zur Produktentwicklung, von internen Kommunikationswegen bis zu externen Dienstleistungsschnittstellen: Nahezu alle Unternehmensbereiche sind digitalisiert. Ein Ausfall dieser Systeme durch Cyberangriffe kann zu erheblichen Verlusten führen, die weit über finanzielle Schäden hinausgehen. Reputationsschäden, der Verlust von Kundenvertrauen und rechtliche Konsequenzen sind nur einige der gravierenden Folgen. Cyberkriminalität ist längst zu einer professionell geführten Industrie geworden, in der hochentwickelte Angriffsmethoden zum Einsatz kommen.

Laut einer Studie des Digital-Branchenverbands Bitkom entstanden der deutschen Wirtschaft im vergangenen Jahr durch Diebstahl von IT-Ausrüstung und Daten sowie durch Industriespionage und Sabotage Schäden in Höhe von 206 Milliarden Euro, davon allein 148 Milliarden Euro durch Cyberattacken. Im Lagebericht für das Jahr 2023 kommt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zum selben alarmierenden Ergebnis: Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Die fortschreitende Digitalisierung und zunehmende Vernetzung vergrößern die Angriffsflächen – und diese werden genutzt.

Herausforderungen auch für die VoIP-Technologie

Besonders die zunehmende Verbreitung von VoIP-Lösungen stellt Unternehmen vor neue Herausforderungen. Verfügbarkeit, Integrität und Vertraulichkeit der Kommunikation sind potenzielle Angriffsziele. Das Problem: Produkte und Lösungen, die für die Sprachkommunikation eingesetzt werden, sind oftmals noch nicht im Bewusstsein der Anwender. Hier werden Sicherheitslücken jedoch ebenso gnadenlos ausgenutzt!

Gleichzeitig zeigt sich, dass viele Unternehmen Schwachstellen aufweisen, weil sie entweder veraltete Sicherheitssysteme einsetzen oder ihre Schutzmaßnahmen nicht kontinuierlich an neue Bedrohungsszenarien anpassen.

Bei Cyberangriffen mit Ransomware (Erpressungssoftware) beobachtet das BSI zudem eine Verlagerung der Attacken: Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Fokus, sondern zunehmend auch kleine und mittelständische Unternehmen sowie staatliche Einrichtungen und Kommunen. Dabei öffnet sich die Schere zwischen großen und kleinen Unternehmen immer weiter: Große Unternehmen haben seit der Pandemie ihr Risikobewusstsein geschärft, während kleineren Unternehmen oft die Zeit und die Ressourcen fehlen, sich umfassend vorzubereiten.

Business Security ist im Übrigen nicht nur eine Frage der Risikominderung; es ist eine grundlegende Voraussetzung für den Geschäftserfolg im 21. Jahrhundert. Kunden, Partner und Regulierungsbehörden erwarten von Unternehmen, dass sie verantwortungsvoll mit Daten umgehen und ihre IT-Infrastruktur gegen Angriffe absichern. Regulatorische Anforderungen, wie sie etwa durch die Datenschutz-Grundverordnung (DSGVO) in Europa gesetzt werden, erhöhen den Druck auf Unternehmen, ihr Sicherheitsniveau zu verbessern.

Höchste Zeit also, dem Thema Business Security noch mehr Aufmerksamkeit zu schenken.

Hätten Sie's gewusst? Das schwächste Glied in der Security-Kette ist der (nicht informierte) Mensch. Laut einer Umfrage von Statista schätzen Arbeitnehmerinnen und Arbeitnehmer in Deutschland ihre Kompetenz im Bereich IT-Sicherheit selbst eher gering ein:

67,7 % *sehr geringe bis mittlere Kompetenz*

32,3 % *große bis sehr große Kompetenz*

Quelle: *Statista im Auftrag von G DATA aus Report: Cybersicherheit in Zahlen 2023, 3. Auflage*

02

Aktuelle Herausforderungen und neue Risiken: Wissen ist Macht

Cyberkriminalität hat viele Gesichter

In einer Welt, in der Cyberbedrohungen zu einer alltäglichen Realität geworden sind, ist es für Organisationen aller Größen und Branchen unerlässlich, sich gegen aktuelle Risiken zu wappnen. Das Problem: Was gestern noch als sicher galt, kann heute schon das Einfallstor für einen Angriff sein. Das Wissen um die aktuellen Herausforderungen und Risiken ist daher der entscheidende Faktor für die Stärkung der eigenen Business Security.

Das Quartett der digitalen Bedrohungen

1 Phishing

Diese raffinierte Taktik verleitet Mitarbeiter dazu, vertrauliche Informationen preiszugeben oder schädliche Anhänge zu öffnen. Die Komplexität dieser Angriffe nimmt ständig zu.

2 Malware

Als Sammelbegriff für schädliche Software umfasst Malware ein breites Spektrum an Bedrohungen. Besonders gefährlich ist Ransomware, die Daten verschlüsselt und Lösegeld fordert, mit potenziell verheerenden Folgen für Unternehmen.

3 Insider Threats

Diese oft unterschätzte Gefahr kommt von innen. Ob durch unzufriedene Mitarbeiter oder unbeabsichtigte Fehler, interne Bedrohungen sind besonders tückisch, da sie schwer zu erkennen sind.

4 DDoS-Angriffe

Statt auf Datendiebstahl oder -manipulation zielen DDoS-Attacken darauf ab, Server oder Netzwerke zu überlasten und Dienste lahmzulegen. Dies öffnet Türen für weitere Angriffe und macht die Abwehr von DDoS-Attacken zu einem kritischen Bestandteil moderner Cybersicherheitsstrategien.

Angriffsvektoren im Wandel – von IoT bis Homeoffice

Während der technologische Fortschritt Unternehmen viele Vorteile in puncto Effizienz und globaler Vernetzung bringt, öffnet er jedoch gleichzeitig neue Türen für Cyberkriminelle:

- **Cloud Computing** bietet Flexibilität, erfordert aber neue Sicherheitskonzepte für Daten außerhalb traditioneller Netzwerkgrenzen.
- **Internet of Things (IoT)** integriert zahlreiche, oft unzureichend gesicherte Geräte in das Unternehmensnetzwerk und schafft potenzielle Einfallstore.
- **Mobile Geräte** und BYOD-Richtlinien (Bring Your Own Device) erweitern das zu schützende Netzwerk um die privaten Geräte der Mitarbeitenden.
- **Homeoffice-Lösungen** verlagern Arbeitsprozesse in potenziell unsichere häusliche Umgebungen.

Für den Unternehmenserfolg ist es entscheidend, technologische Trends und deren Sicherheitsrisiken frühzeitig zu erkennen und proaktiv zu handeln. Ein fundiertes Verständnis aktueller und zukünftiger Cyberbedrohungen kann den entscheidenden Vorsprung in der Unternehmensabsicherung bedeuten.

Und was ist eigentlich SD-WAN?

SD-WAN (Software-Defined Wide Area Network) ist ein fortschrittlicher Ansatz, um Unternehmensnetzwerke über große Distanzen hinweg zu verbinden. Statt herkömmlicher Router nutzt SD-WAN Software, um den Netzwerkverkehr zu steuern, was mehr Flexibilität und Kontrolle ermöglicht. Durch die zentrale Managementfähigkeit von SD-WAN können Sicherheitsrichtlinien über verschiedene Standorte und Cloud-Dienste effizient angewendet werden.

Das ist besonders vorteilhaft für Teams im Homeoffice, weil es dabei hilft, die gleichen Sicherheitsstandards wie im Firmennetzwerk zu gewährleisten. SD-WAN sorgt für einen verschlüsselten Datenverkehr und bietet durch integrierte Sicherheitsfunktionen wie Firewalls einen zusätzlichen Schutz vor Cyberangriffen. Unterm Strich trägt SD-WAN dazu bei, dass Ihr Unternehmen sicher und verbunden bleibt – eine wichtige Säule in einer zunehmend vernetzten Geschäftswelt.

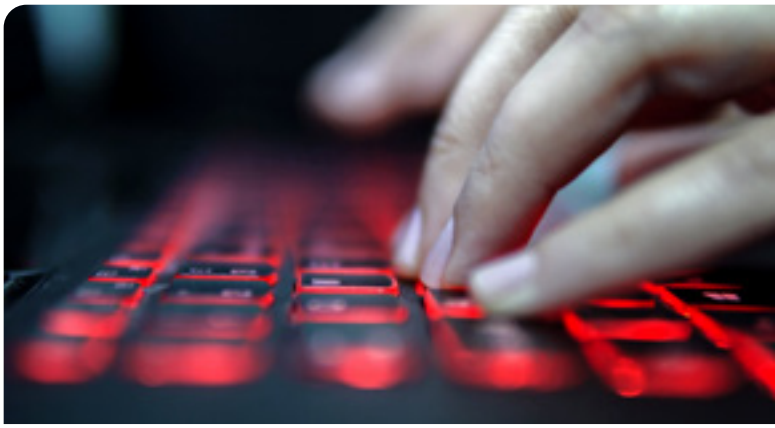
Realitätscheck oder „the struggle is real“: Unternehmen im Visier von Cyberangriffen

03

Virtuelle Bedrohungen mit realen Folgen: die globale Cyberangriffswelle und ihre Auswirkungen

Berichte über Hackerangriffe sind inzwischen fast alltäglich, ihre konkrete Bedeutung und volle Tragweite bleiben jedoch oft im Verborgenen. Doch die Wirklichkeit zeigt: Cyberangriffe treffen Organisationen aller Größenordnungen und die Folgen können dramatisch sein, wie es einer der größten DDoS-Angriffe der Geschichte gezeigt hat.

Hackerangriff auf die Stadtverwaltung von Rodgau



Cyberkriminelle legten Ende Februar 2024 die Computersysteme der Stadtverwaltung Rodgau lahm und entwendeten rund ein Terabyte an Daten. Der Angriff zwang die Stadtverwaltung, die Stadtwerke und Kindertagesstätten dazu, vorübergehend auf Papier und Bleistift umzusteigen. Obwohl keine Meldungen über Missbrauch der entwendeten Daten vorliegen, führte das zu erheblichen Beeinträchtigungen des täglichen Betriebs. Die Sicherheitsmaßnahmen wurden verschärft, allerdings war der Zeitpunkt der vollständigen Wiederherstellung der Systeme lange ungewiss.

Die Ransomware-Attacke auf die Südwestfalen-IT

Der Cyberangriff der Hackergruppe Akira auf die Südwestfalen-IT im Jahr 2023 zählt zu den schwersten Cyberangriffen in Deutschland und legte die IT-Infrastruktur von 72 Kommunen in Nordrhein-Westfalen lahm, wobei über 103 Stadt- und Kreisverbände betroffen waren. Dies hatte massive Auswirkungen auf öffentliche Dienstleistungen: Die Ausstellung von Dokumenten wie Pässen und Führerscheinen war gestört, die Auszahlung von Sozialleistungen verzögerte sich, und die Stadt Bergisch Gladbach konnte wegen des Angriffs keine Gewerbesteuern einziehen. Noch Monate nach dem Vorfall arbeiteten mehr als 170 Experten an der Wiederherstellung der IT-Systeme.

Der Mirai-Angriff oder *„Der Zusammenbruch des Internets“*

Die DDoS-Attacke, verursacht durch das Mirai-Botnet, zählt zu den verheerendsten Angriffen in der Geschichte der Cyberkriminalität. Die Malware infizierte im Oktober 2016 eine gigantische Anzahl von mit dem Internet verbundenen Geräten, insbesondere solche, die unzureichend gesichert waren (Benutzernamen und Passwörter!), wie IP-Kameras, Heimrouter und andere IoT-Geräte und verband sie zu einem Netzwerk von „Bots“ (Botnet). Die Kontrolle über Hunderttausende von Geräten wurde anschließend dazu benutzt, massiven Traffic auf die Server von Dyn, einem Unternehmen, das Domain-Name-System(DNS)-Dienstleistungen anbietet, zu leiten. Der DDoS-Angriff auf Dyn hatte zur Folge, dass viele populäre Websites und Dienste wie Twitter, Netflix, Reddit und viele andere, die auf die Dienste von Dyn angewiesen sind, stundenlang nicht oder nur stark eingeschränkt erreichbar waren.

04

Best Practices für Präventionsmaßnahmen und deren Umsetzung

Schutzmaßnahmen gegen Cyberkriminalität

Die Zeiten, in denen IT-Sicherheit lediglich eine technische Angelegenheit war, sind offensichtlich vorbei – heute hat sie strategische Priorität. Die Gefahrenpotenziale sind vielfältiger und komplexer geworden, die Bedrohung ist global, unerbittlich und entwickelt sich ständig weiter. Kein Unternehmen kann es sich leisten, vor dieser Realität die Augen zu verschließen. Die Frage ist nicht mehr, ob, sondern wann es zu einem Angriff kommt.

Die fünf Säulen einer robusten Cybersicherheitsstrategie

Von der Etablierung einer robusten Sicherheitskultur über die Identifizierung und Bewertung von Risiken bis hin zu präventiven und reaktiven Sicherheitsmaßnahmen: Das hier sollten Unternehmen unbedingt wissen – und natürlich auch umsetzen:

1. **Sicherheitskultur etablieren:** Eine effektive Cybersicherheitsstrategie erfordert die Verankerung einer starken Sicherheitskultur im Unternehmen, z. B. durch konkrete Investitionen in Sicherheitsinitiativen und die Verankerung von Sicherheitswerten in der Unternehmensmission. Wichtig ist, dass die Sicherheitskultur von allen Mitarbeitern gelebt wird, was durch regelmäßige Schulungen, klare Kommunikationskanäle und die Integration von Sicherheitspraktiken in den Arbeitsalltag erreicht wird.

2. **Risikomanagement einführen:** Unternehmen müssen ihre spezifischen Risiken kennen und verstehen. Eine gründliche Bestandsaufnahme der IT-Infrastruktur und aller wichtigen Komponenten ist daher unerlässlich, um Schwachstellen zu erkennen. Neben der Erfassung der Risiken ist die Bewertung hinsichtlich der Eintrittswahrscheinlichkeit und des potenziellen Schadens entscheidend. Ein ausgereiftes Risikomanagement beinhaltet mehrdimensionale Ansätze, die dynamisch angepasst und durch neueste Technologien wie Künstliche Intelligenz unterstützt werden. Entscheidend für den Erfolg ist dabei die kontinuierliche Anpassung und Überprüfung des Risikomanagementplans.

3. **Technische Sicherheitsmaßnahmen stärken:** Im Zentrum des technischen Schutzes steht eine robuste Netzwerksicherheitsarchitektur, ergänzt durch Firewalls, Intrusion-Detection-Systeme (Programme, die überwachen, ob jemand unbefugt in das System eindringt) und fortschrittliche Malware-Erkennung. Sicherheitsstandards wie Verschlüsselung und Multi-Faktor-Authentifizierung tragen zur Integrität der Daten bei. Automatisierte Sicherheitssysteme und das zügige Beheben von Software-Schwachstellen sind unerlässlich, um auf Bedrohungen schnell reagieren zu können. Der fortlaufende Prozess der technischen Absicherung muss eine flexible Anpassung an neue Technologien und Bedrohungsszenarien ermöglichen.

4. **Vorbereitung auf Sicherheitsvorfälle:** Ein wesentlicher Bestandteil der Unternehmenssicherheit ist die Fähigkeit, auf IT-Sicherheitsvorfälle angemessen reagieren zu können. Ein gut vorbereiteter Incident Response Plan (Notfallplan für den Ernstfall) ermöglicht eine rasche und koordinierte Reaktion auf Sicherheitsvorfälle und definiert die notwendigen Schritte, die im Falle eines Sicherheitsvorfalls zu setzen sind. Im Mittelpunkt des Notfallmanagements steht ein speziell geschultes interdisziplinäres Team, das im Ernstfall die Koordination übernimmt. Eine gute Vorbereitung umfasst klar formulierte Anweisungen für die Eskalation, Kommunikation und Dokumentation des Vorfalls sowie definierte Prozesse zur Wiederherstellung der Systeme nach einem Angriff.

5. **Compliance und rechtliche Anforderungen identifizieren und einhalten:** Die Compliance mit Datenschutz- und Sicherheitsvorschriften ist mehr als eine Pflichtübung, sie schützt vor Bußgeldern und stärkt das Vertrauen der Stakeholder. Unternehmen müssen sich nicht nur an allgemeine Regelwerke wie die DSGVO, sondern auch an branchenspezifische Vorgaben halten. Erforderlich ist ein systematischer Ansatz, der Datenschutz und Compliance in die Unternehmensstrategie integriert. Die Benennung eines Datenschutzbeauftragten und regelmäßige Compliance-Audits stellen sicher, dass die gesetzlichen Vorgaben eingehalten werden.

Was Sie über die NIS-2-Richtlinie wissen sollten

Die NIS-2-Richtlinie ist eine wichtige EU-Verordnung, die eine robuste Cyber- und Informationssicherheit für Unternehmen und Institutionen vorschreibt. Sie ersetzt die ältere NIS-Richtlinie aus dem Jahr 2016 und soll das Sicherheitsniveau in den EU-Mitgliedstaaten durch eine Verschärfung der Cybersicherheitsanforderungen erhöhen. Mit ihrer Veröffentlichung im Dezember 2022 und ihrem Inkrafttreten im Januar 2023 müssen die EU-Mitgliedstaaten bis Oktober 2024 entsprechende nationale Rechtsvorschriften schaffen, um die neuen Anforderungen umzusetzen.

Was ändert sich? NIS-2 weitet die Anforderungen und Sanktionen deutlich aus, betrifft mehr Branchen und Unternehmen als bisher und stellt strengere Anforderungen an das Risikomanagement, die Kontroll- und Überwachungssysteme sowie die Meldepflichten bei Sicherheitsvorfällen. Auch die Unternehmensleitung wird stärker in die Verantwortung genommen und muss entsprechende Schulungen anbieten und durchführen.

Warum ist dies für Unternehmen relevant? Angesichts des wachsenden Risikos von Cyberangriffen und der Bedeutung von IT-Sicherheit können die Folgen einer Nichteinhaltung gravierend sein – von hohen Bußgeldern bis hin zur persönlichen Haftung der Verantwortlichen bei Sicherheitsvorfällen. Unternehmen müssen sich daher rechtzeitig mit NIS-2 auseinandersetzen, um die Anforderungen zu verstehen, entsprechende Maßnahmen zu ergreifen und somit sicherzustellen, dass sie im Einklang mit den neuen Regelungen handeln.

Der Schlüsselpartner für Ihre Sicherheit

05

Der Telekommunikationsanbieter: unverzichtbarer Verbündeter im Kampf gegen Cyberbedrohungen

Mit der zunehmenden Komplexität von Cyberbedrohungen wird auch die Rolle des richtigen Telekommunikationsanbieters immer wichtiger. Die frühere Trennung zwischen der Bereitstellung von Konnektivität und der Gewährleistung der Datenintegrität verschwimmt. Heute ist der Provider nicht nur ein wichtiger Schnittstellenpartner in der digitalen Infrastruktur von Unternehmen, sondern auch der erste Verteidiger gegen cyberkriminelle Aktivitäten.

Partners in Crime – die Allianz zwischen Telekommunikationsanbietern und Unternehmen

Infrastruktur und Netzwerksicherheit: Telekommunikationsanbieter stellen die Basisinfrastruktur für die digitale Kommunikation bereit. Sie bieten sichere Netzwerkverbindungen wie Virtual Private Networks (VPNs) an und implementieren fortgeschrittene Technologien wie Ende-zu-Ende-Verschlüsselung, um den Datenverkehr vor unberechtigten Zugriffen und Cyberspionage zu schützen.

Robustheit und Verfügbarkeit: Gerade in Zeiten der Digitalisierung ist die Zuverlässigkeit der IT-Infrastruktur entscheidend. Telekommunikationsanbieter stellen eine hohe Verfügbarkeit der Netzdienste sicher und minimieren so das Risiko von Ausfallzeiten, was für Geschäftsprozesse und die Aufrechterhaltung des Geschäftsbetriebs unerlässlich ist.

Managed Security Services: Viele Anbieter haben Managed Security Services in ihr Portfolio aufgenommen. Sie überwachen Netzwerk- und Systemaktivitäten, identifizieren Bedrohungen in Echtzeit durch fortschrittliche Gefahrenerkennung, stellen Incident-Response-Pläne bereit und bieten regelmäßige Sicherheitsaudits und Compliance-Beratung.

Datensicherheit und Compliance: Strenge Datenschutzgesetze wie die EU-Datenschutz-Grundverordnung (DSGVO) verlangen von Unternehmen, dass ihre Daten sicher verarbeitet und gespeichert werden. Telekommunikationsanbieter unterstützen die Einhaltung dieser Vorschriften durch zertifizierte Prozesse und Datenmanagement-Technologien.

Beratung und Unterstützung: Der Digitalisierungsprozess bringt neue und komplexe Herausforderungen mit sich, darunter die Auswahl der richtigen Technologie und das Management von Cyberrisiken. Telekommunikationsanbieter bieten fachkundige Beratung, um Unternehmenskunden bei diesen Entscheidungen zu unterstützen und Risiken zu minimieren.

Partnerschaft und Integration: Telekommunikationsanbieter arbeiten häufig mit Drittanbietern und Sicherheitsexperten zusammen, um integrierte Sicherheitslösungen anzubieten. Auf diese Weise können Unternehmen von einer umfassenden Sicherheitsstrategie profitieren, die über grundlegende Telekommunikationsdienste hinausgeht.

Skalierbarkeit und Flexibilität: In einem dynamischen Geschäftsumfeld müssen Unternehmen schnell auf Veränderungen reagieren können. Telekommunikationsanbieter bieten skalierbare Lösungen an, die mit den Anforderungen eines Unternehmens wachsen und sich anpassen können, ohne die Sicherheit zu vernachlässigen.

Telekommunikationsanbieter sind Ihre Frontlinie gegen Cyberbedrohungen. Mit hochmodernen Sicherheitslösungen schützen sie Ihr Unternehmen vor digitalen Gefahren. Als zuverlässiger Partner bieten sie nicht nur robuste Infrastruktur, sondern auch maßgeschneiderte Sicherheitsdienste, Compliance-Unterstützung und zukunftssichere Flexibilität.

Besser von Anfang an mitdenken: Sicherheit für Ihre VoIP-Kommunikation

Wie eingangs erwähnt, erweist sich insbesondere die rasante Verbreitung von VoIP-Technologien für viele Unternehmen als wahres Minenfeld. Interessant dabei ist, dass die Anwender oft blindlings in die Fallen der modernen Sprachkommunikation tappen, weil schlicht und ergreifend das Wissen um die Schwachstellen der eingesetzten Produkte und Lösungen fehlt. Dabei werden selbst kleinste Sicherheitslücken von Cyberkriminellen ohne Zögern und mit verheerenden Folgen ausgenutzt.

In der digitalen Welt ist Sicherheit aber nicht verhandelbar – gerade wenn es um geschäftliche Kommunikationskanäle geht. Deshalb bietet M-net seinen Kunden einen BSI-konformen SIP-Trunk, der Sicherheit auf höchstem Niveau bietet. Als KRITIS-Unternehmen stellt M-net sicher, dass seine Dienste gegen verschiedenste Cyberangriffe geschützt sind. Der M-net SIP-Trunk erfüllt alle Voice-spezifischen Voraussetzungen der Technischen Richtlinie des BSI (TL-02103) sowie des IT-Grundschutzes.

Dazu gehören neben robusten physikalischen und logischen Schutzmaßnahmen auch systemische Sicherungen zum Schutz vor Cyberangriffen, Hacking und Sabotage. Der M-net SIP-Trunk bietet zwar bereits einen hervorragenden Schutz für Ihre Daten. Um jedoch auch auf Ihrer Seite eine Sicherheitsinfrastruktur nach den Vorgaben des BSI zu gewährleisten, ist Ihre Mitwirkung entscheidend.

M-net unterstützt Sie unkompliziert bei der Zertifizierung Ihrer Telekommunikationslösung nach BSI-Konformität und entwickelt gemeinsam mit Ihnen eine optimale Sicherheitsstrategie für Ihre VoIP-Kommunikation.

Ihre Vorteile

Guter Schutz als Standard
M-net bietet Ihnen bereits in der Standardausstattung Ihres SIP-Trunk-Vertrages einen umfassenden Schutz vor sogenannten Telefonie-DoS-Attacken (Denial of Service).

Verschlüsselungslösungen
M-net bietet kostenlose und einfach zu implementierende Verschlüsselungslösungen für Ihren SIP-Trunk.

Access-Anforderungen
Qualität und Priorisierung Ihrer Gespräche werden auf M-net Internet-Anschlüssen mit VoIP-Ready sichergestellt. Zur weiteren Risikominimierung bietet M-net explizite VoIP-only-Konfigurationen an.

Backup-Lösungen
Die Implementierung redundanter Zugangs- und Systemlösungen stellt sicher, dass Ihre Infrastruktur im Notfall über alternative Kommunikationswege verfügt.

06

Zukunft der Cyber-kriminalität und Business Security: die Rolle der KI

Künstliche Intelligenz: Wegbereiter und Heraus-forderung für die Cybersicherheit der Zukunft

In einer Zeit zunehmender digitaler Vernetzung und wachsender technologischer Abhängigkeit rückt die Cybersicherheit in den Mittelpunkt unternehmerischer Aufmerksamkeit. Die Integration von Künstlicher Intelligenz (KI) in diesem Bereich eröffnet sowohl faszinierende Möglichkeiten als auch neue Risikodimensionen, die es sorgfältig abzuwägen gilt.

Revolution mit Risiken

KI-Systeme revolutionieren die Cybersicherheit durch ihre Fähigkeit, komplexe Datenmengen in Echtzeit zu analysieren, subtile Muster zu erkennen und Anomalien aufzuspüren – Aufgaben, die die menschliche Wahrnehmung oft übersteigen. Diese digitalen Wächter ermöglichen eine proaktive Abwehr von Cyberangriffen und eine tiefgreifende Analyse von Bedrohungsszenarien. Doch wie jede bahnbrechende Technologie ist auch KI ein zweischneidiges Schwert: In den Händen von Cyberkriminellen kann sie zu einem mächtigen Werkzeug werden, um Sicherheitssysteme zu unterwandern und neue Angriffsmethoden zu entwickeln. Gleichzeitig besteht die Gefahr, dass KI-gestützte Sicherheitssysteme selbst zur Zielscheibe werden – etwa durch raffinierte Manipulationstechniken wie „Adversarial Learning", die darauf abzielen, die KI in die Irre zu führen.

Die Integration von KI in die Cybersicherheit erfordert daher nicht nur technisches Know-how, sondern auch ein ausgeprägtes ethisches Bewusstsein. Es muss ein Rahmen geschaffen werden, der Missbrauch verhindert und unbeabsichtigte negative Folgen minimiert. Nur durch ein tiefgreifendes Verständnis der Technologie, ihrer Potenziale und Grenzen sowie durch ständige Wachsamkeit und Anpassungsfähigkeit können Unternehmen die Chancen von KI in der Cybersicherheit voll ausschöpfen und gleichzeitig die damit verbundenen Risiken beherrschen.

Aha, aha!

Schon gewusst? Die Grundlagen der Künstlichen Intelligenz (KI) wurden bereits in den 1940er Jahren gelegt! Damals entwarfen die beiden Wissenschaftler Warren McCulloch und Walter Pitts das Konzept der „künstlichen neuronalen Netze". Diese Netzwerke, die sich an der Struktur des menschlichen Gehirns orientieren, bestehen aus einer Vielzahl miteinander verbundener Knoten und sind in der Lage, durch die Verarbeitung von Daten zu lernen. Dieses innovative Denkmodell bildete den Ausgangspunkt für die Entwicklung der heutigen Künstlichen Intelligenz, die auf einem ähnlichen Prinzip beruht.

Vorsprung durch Sicherheit: Ihr Weg in eine sichere Zukunft beginnt jetzt

07

Das Motto? Proaktiv statt reaktiv!

Angesichts der immer raffinierteren und vielfältigeren Cyberbedrohungen ist es entscheidend, dass Sie Ihr Unternehmen aktiv schützen. Es reicht längst nicht mehr aus, nur auf Sicherheitsvorfälle zu reagieren. Vielmehr gilt es, eine umfassende Sicherheitsstrategie zu entwickeln und konsequent umzusetzen.

Und wie geht das? Ganz einfach Schritt für Schritt

- Machen Sie Sicherheit zur Chefsache: Integrieren Sie Cybersecurity in Ihre Unternehmensstrategie und -kultur.
- Investieren Sie in Ihr wichtigstes Kapital: Schulen Sie Ihre Mitarbeiterinnen und Mitarbeiter regelmäßig und umfassend.
- Bleiben Sie wachsam: Implementieren Sie ein proaktives Risikomanagement und passen Sie es kontinuierlich an.
- Rüsten Sie technologisch auf: Setzen Sie auf moderne Sicherheitslösungen und halten Sie diese stets aktuell.
- Planen Sie für den Ernstfall: Entwickeln Sie robuste Notfallpläne und testen Sie diese regelmäßig.
- Suchen Sie sich starke Partner: Arbeiten Sie mit erfahrenen Sicherheitsexperten zusammen, um Ihre Abwehr zu stärken.

Eine Investition in Cybersecurity ist eine Investition in die Zukunftsfähigkeit Ihres Unternehmens. Sie schützt nicht nur Ihre Daten und Systeme, sondern auch das Vertrauen Ihrer Kunden und Partner. Cybersecurity ist nicht länger optionale Komponente, sondern eine zwingende Grundvoraussetzung für den Geschäftserfolg in einer zunehmend digitalisierten Welt. Sicherheitsverletzungen sind nicht nur theoretische Risiken, sondern konkrete und kostenintensive Bedrohungen. **Die Entwicklung einer ganzheitlichen und proaktiven Sicherheitsstrategie, die menschliches Handeln, technische Lösungen und organisatorische Maßnahmen umfasst, ist von zentraler Bedeutung.** Cybersecurity muss integraler Bestandteil jeder Unternehmenskultur werden. Nur so können Unternehmen den Herausforderungen von heute und morgen sicher und kraftvoll begegnen.

Ihre Sicherheit ist unser wichtigstes Anliegen!
Kontaktieren Sie uns für eine unverbindliche Beratung.

Telefon **0800 7239848**
oder hier direkt kontaktieren: **m-net.de/gk-kontakt**

Mehr zu den M-net Security-Lösungen
erfahren Sie unter:

m-net.de/business-security

M-net Telekommunikations GmbH
Business Unit Geschäftskunden
Frankfurter Ring 158
80807 München

M·net