AQ SECURE

EMPFEHLUNGEN ZUR CYBERSICHERHEIT FÜR KLEINE UND MITTLERE UNTERNEHMEN IM ZEITALTER DER KI

AQ SECURE

EMPFEHLUNGEN ZUR CYBERSICHERHEIT FÜR KLEINE UND MITTLERE UNTERNEHMEN IM ZEITALTER DER KI

1. EINLEITUNG: UMFASSENDE CYBERSICHERHEIT IST FÜR KLEINE UND MITTLERE UNTERNEHMEN UNVERZICHTBAR

In der Vergangenheit wurden Cyberangriffe primär mit großen Unternehmen assoziiert, die aufgrund ihres hohen Wertes und ihrer umfangreichen Datenbestände als primäre Ziele galten. Doch die aktuellen Studien, wie beispielsweise die Cybercrime-Studie von Accenture, belegen, dass 43 Prozent aller Cyberangriffe gezielt auf kleine und mittlere Unternehmen (KMU) gerichtet sind.

Diese Entwicklung unterstreicht eine alarmierende Veränderung im Bedrohungsbild: KMU sind heute keine Nebenakteure mehr, sondern stehen im Zentrum des Interesses von Cyberkriminellen.

Der Hauptgrund für diese Verschiebung liegt in einer kritischen Schwachstelle. Lediglich 14 Prozent der KMU sind adäquat auf die Abwehr von Cyberangriffen vorbereitet. Diese mangelnde Vorbereitung macht sie zu idealen und verlockenden Zielen.

Die Konsequenzen eines erfolgreichen Angriffs auf ein KMU können verheerend sein, angefangen von finanziellen Einbußen über den Verlust von Kundendaten und Reputationsschäden bis hin zur vollständigen Betriebsunterbrechung.

Cyberkriminelle haben außerdem ihre Angriffsstrategien diversifiziert und setzen längst nicht mehr ausschließlich auf hochkomplexe, gezielte Angriffe, die spezifisches Know-how erfordern. Stattdessen nutzen sie verstärkt automatisierte Methoden, die eine breite Streuung und hohe Effizienz ermöglichen.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Dazu gehören automatisierte Scans von Netzwerken und IT-Systemen auf Schwachstellen, breit gestreute Phishing-Kampagnen, die darauf abzielen, Zugangsdaten oder andere sensible Informationen zu erbeuten, sowie der Einsatz von Ransomware-as-a-Service (RaaS)-Angeboten. Diese Dienste ermöglichen es auch weniger technisch versierten Angreifern, erpresserische Schadsoftware einzusetzen. Das Perfide daran ist, dass bei diesen Massenangriffen kein Unterschied hinsichtlich der Unternehmensgröße gemacht wird.

Im Gegenteil, KMU werden oft als besonders anfällig eingestuft, da ihnen im Vergleich zu Großunternehmen häufig die notwendige Zeit, das spezifische Know-how und die erforderlichen finanziellen Ressourcen fehlen, um moderne und effektive Abwehrmechanismen zu implementieren und kontinuierlich zu pflegen.

Viele KMU verharren in einer trügerischen Sicherheit, indem sie sich auf klassische Antivirenlösungen verlassen, die nur einen Bruchteil der heutigen Bedrohungslandschaft abdecken können.

Eine weitere weit verbreitete, aber gefährliche Annahme ist die Überzeugung, für Cyberkriminelle "uninteressant" zu sein. Dies ist jedoch ein gravierender Irrtum. Unabhängig von der Firmengröße sind Daten, Kundeninformationen, Betriebsgeheimnisse und die IT-Infrastruktur selbst von erheblichem Wert. Sie stellen begehrte Angriffsziele dar, da sie entweder direkt monetarisiert (z. B. durch Datenverkauf oder Erpressung) oder als Sprungbrett für weitere Angriffe genutzt werden können.

Darüber hinaus bringt die zunehmende Integration von Künstlicher Intelligenz (KI) und KI-gestützten Lösungen in Geschäftsprozessen zur Automatisierung, Entscheidungsunterstützung und Betriebsoptimierung neue Komplexitäten und Risiken mit sich. KI bietet zwar erhebliches Innovations- und Effizienzpotenzial, verarbeitet aber auch hochsensible Informationen wie Kundendaten, Quellcode oder Finanzinformationen, die bei der Analyse und Nutzung umfassenden Schutz erfordern. KI-Systeme, insbesondere Machine-Learning-Modelle, sind neuartigen Angriffsformen ausgesetzt, die über traditionelle Cybersicherheitsbedenken hinausgehen.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Aus diesen Gründen ist Cybersicherheit heute keine optionale Kür mehr, sondern eine zwingende Pflicht für jedes KMU. Wer seine Geschäftsprozesse, die Integrität seiner Mitarbeitenden und die Vertrauensbeziehungen zu seinen Kunden nachhaltig absichern möchte, benötigt in der heutigen digitalen Ära eine umfassende, ganzheitliche Sicherheitsstrategie. Diese Strategie muss nicht nur effektiv sein, sondern auch einfach in der Handhabung, effizient in der Umsetzung und spezifisch auf die Realität und die Bedürfnisse KMU zugeschnitten sein, um praktikabel zu sein und den maximalen Schutz zu gewährleisten.

2. CYBERSICHERHEITS-HERAUSFORDERUNGEN DER KMU

Kleine und mittlere Unternehmen sehen sich einem fundamentalen Dilemma gegenübergestellt, das die Cybersicherheit maßgeblich beeinflusst. Während ihre digitale Angriffsfläche bedingt durch die zunehmende Digitalisierung von Geschäftsprozessen, die Nutzung von Cloud-Diensten, KI-Lösungen und die Einführung flexibler Arbeitsmodelle stetig expandiert, bleiben die personellen und finanziellen Ressourcen, die für eine adäquate Cybersicherheit zur Verfügung stehen, in den meisten Fällen begrenzt. Dies schafft eine gefährliche Asymmetrie, die KMU besonders anfällig für Cyberangriffe macht.

Die typischen Herausforderungen, denen sich KMU in diesem Kontext stellen müssen, sind vielschichtig und bedürfen einer genauen Betrachtung:

Wenige oder keine dedizierten IT-Sicherheitsverantwortlichen

In vielen KMU wird die IT-Verwaltung häufig „nebenbei“ von Mitarbeitenden mit anderen Kernaufgaben übernommen, häufig von Generalisten oder der Geschäftsführung selbst, die keine spezialisierte Ausbildung oder ausreichende Zeit für IT-Sicherheit haben.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

IT-Sicherheit wird dabei oft als ein zusätzliches Thema betrachtet, das ad-hoc behandelt wird, anstatt als strategischer Schwerpunkt, der kontinuierliche Aufmerksamkeit und spezialisiertes Fachwissen erfordert. Dies führt zu Wissenslücken, einer reaktiven statt proaktiven Sicherheitshaltung und dem Übersehen kritischer Sicherheitsaspekte.

Zunehmend dezentrale Arbeitsweisen

Die Zunahme von Telearbeit und Homeoffice-Modellen hat die traditionellen Perimeter der Unternehmensnetzwerke aufgelöst. Mitarbeitende greifen von unterschiedlichen Standorten auf Unternehmensressourcen zu, oft über private Geräte (Bring Your Own Device – BYOD) oder ungeschützte öffentliche Netzwerke. Diese dezentrale Arbeitsweise erhöht die Komplexität der Cybersicherheitsarchitektur erheblich und schafft zahlreiche neue Angriffsvektoren, da die Kontrolle über die Endpunkte und die Netzwerkumgebung außerhalb des direkten Einflusses des Unternehmens liegt.

Vielseitige, schwer erkennbare Cyberbedrohungen

Die Landschaft der Cyberbedrohungen ist dynamisch und entwickelt sich ständig weiter. Phishing-E-Mails sind immer raffinierter und kaum von echten Nachrichten zu unterscheiden. Infizierte Webseiten, schädliche Downloads, die sich als legitime Software tarnen, oder manipulierte Cloud-Logins wirken oft täuschend echt und sind für ungeschulte Augen nur schwer zu identifizieren.

KMU fehlt es oft an den notwendigen Technologien (z. B. fortschrittliche Erkennungssysteme, Bedrohungsanalyse-Plattformen) und dem Fachpersonal, um diese subtilen und oft sehr gezielten Angriffe frühzeitig zu erkennen und abzuwehren.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Aufwendige Updates und Einhaltung von Richtlinien

Die kontinuierliche Pflege von Software, Geräten, Benutzerrechten und Sicherheitsrichtlinien ist eine zeitintensive und komplexe Aufgabe. Regelmäßige Updates und Patches sind unerlässlich, um bekannte Schwachstellen zu schließen, doch ohne eine zentrale Steuerung und Automatisierung wird diese Aufgabe schnell unüberschaubar und fehleranfällig. Die manuelle Verwaltung von Berechtigungen, die Überprüfung der Einhaltung von Richtlinien und die Dokumentation von Prozessen binden Ressourcen, die in KMU typischerweise knapp sind.

Fehlende Übersicht und Reaktion bei Vorfällen

Im Falle eines Cyberangriffs sind Zeit und eine koordinierte Reaktion entscheidend. Viele KMU erkennen Angriffe jedoch zu spät oder reagieren unkoordiniert, weil Warnsignale übersehen, falsch interpretiert oder nicht ernst genug genommen werden. Das Fehlen klar definierter Incident-Response-Pläne, unzureichende Protokollierung und mangelnde Transparenz im Netzwerk verhindern eine schnelle Lokalisierung der Ursache, Eindämmung des Schadens und Wiederherstellung des Betriebs.

Diese Ansammlung von Herausforderungen macht KMU nicht nur besonders verwundbar, sondern leider auch besonders attraktiv für Angreifer.

Die Kombination aus wertvollen Daten und Infrastrukturen auf der einen Seite und begrenzten Abwehrmöglichkeiten auf der anderen Seite schafft ein ideales Umfeld für Cyberkriminelle, ihre Angriffe mit hoher Erfolgswahrscheinlichkeit durchzuführen.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

3. WARUM KLASSISCHE IT-SICHERHEITSANSÄTZE HEUTE NICHT MEHR AUSREICHEN

In vielen KMU sind die IT-Sicherheitsarchitekturen historisch gewachsen, über Jahre hinweg. Dies bedeutet, dass sie häufig auf traditionellen Konzepten und Technologien basieren, die für die Bedrohungslandschaft von gestern entwickelt wurden. Typischerweise umfassen diese Ansätze klassische Firewalls, die den Netzwerkverkehr an den Perimetern filtern, und VPN-Verbindungen (Virtual Private Networks), die einen sicheren Tunnel für den externen Zugriff auf das interne Netzwerk schaffen. Ergänzt werden diese meist durch Antivirensoftware, die auf den Endgeräten installiert ist, um bekannte Malware zu erkennen und zu blockieren. Auf den ersten Blick mag ein solches Setup solide und ausreichend erscheinen. Doch bei genauerer Betrachtung der heutigen, sich rasant entwickelnden Bedrohungslandschaft wird deutlich, dass diese klassischen Ansätze längst nicht mehr ausreichen, um einen umfassenden Schutz zu gewährleisten.

Die Schwachstellen dieser traditionellen Konzepte sind vielfältig:

Unzureichende Phishing-Erkennung

Phishing-Angriffe, die über E-Mail oder infizierte Webseiten erfolgen, werden von klassischen Cybersicherheitslösungen oft nicht oder zu spät erkannt. Diese Cybersicherheitslösungen prüfen selten kontextbezogen oder in Echtzeit. Sie basieren häufig auf statischen Signaturen bekannter Bedrohungen und sind nicht in der Lage, dynamische oder neuartige Phishing-Varianten zu identifizieren, die darauf abzielen, menschliche Fehler auszunutzen.

VPN-Zugänge als breites Einfallstor

Viele traditionelle VPN-Lösungen gewähren Benutzern nach erfolgreicher Authentifizierung oft umfassenden Zugriff auf das gesamte interne Netzwerk. Dies geschieht, ohne dass eine granulare Zugriffskontrolle oder eine Segmentierung des Netzwerks implementiert wäre.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Ein kompromittierter VPN-Zugang kann somit einem Angreifer ermöglichen, sich frei im Unternehmensnetzwerk zu bewegen und auf sensible Daten oder IT-Systeme zuzugreifen, die für die eigentliche Tätigkeit des Benutzers gar nicht erforderlich wären.

Fehlende Migrationsstrategie zu modernen Cybersicherheitsmodellen

Obwohl Cloud-Nutzung und mobile Arbeitsweisen längst zum Alltag geworden sind, fehlt vielen KMU eine Strategie zur Migration hin zu modernen Cybersicherheitsmodellen wie Zero Trust oder Secure Access Service Edge (SASE). Diese Cybersicherheitsmodelle sind darauf ausgelegt, Sicherheit unabhängig vom Standort des Benutzers oder der Ressource zu gewährleisten und basieren auf dem Prinzip "Vertraue niemandem, überprüfe alles". Ohne diese Migration bleiben traditionelle Architekturen unzureichend und unsicher in einer dezentralisierten und cloud-basierten Arbeitswelt.

Überschätzung der Cloud-Sicherheit

Mit der Verlagerung von IT-Infrastruktur in die Cloud werden oft Hardwarekosten reduziert. Doch gleichzeitig wird die Sicherheit oft vernachlässigt oder ihre Verantwortung fälschlicherweise vollständig dem Cloud-Anbieter zugeschrieben. Viele Unternehmen unterschätzen die Notwendigkeit, auch in der Cloud eigene Sicherheitsmaßnahmen zu ergreifen.

Manuelle Prozesse und mangelnde Transparenz

Klassische Ansätze leiden oft unter fehlender oder nur manueller Aktualisierung von IT-Systemen, mangelnder Automatisierung, schwacher Nutzerverwaltung und unzureichender Transparenz im Netzwerk.

Dies macht es schwierig, Sicherheitslücken schnell zu erkennen, auf Vorfälle zu reagieren und eine konsistente Sicherheitsrichtlinie durchzusetzen.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

4. DIE ILLUSION DER VOLLSTÄNDIGEN CLOUD-SICHERHEIT

Ein besonders gefährlicher Irrtum, der sich im Zuge der Cloud-Adoption verbreitet hat, ist die Annahme, dass mit der Auslagerung von Anwendungen und Daten in die Cloud der Cloud-Anbieter automatisch "für alles" zuständig sei. Dieses Missverständnis kann zu gravierenden Sicherheitslücken führen. Tatsächlich basiert Cloud-Sicherheit auf einem geteilten Verantwortungsmodell (Shared Responsibility Model), bei dem sowohl der Cloud-Anbieter als auch der Kunde spezifische Sicherheitsaufgaben übernehmen müssen.

Aufgaben des Cloud-Anbieters

Der Cloud-Anbieter ist primär für die Sicherheit der Cloud-Infrastruktur verantwortlich also für das, "was die Cloud ausmacht". Dazu gehören:

- **Physische Sicherheit:** Schutz der Rechenzentren, der Server, der Netzwerkkomponenten und der gesamten Hardware vor unbefugtem Zugriff, Naturkatastrophen und anderen physischen Bedrohungen.
- **Plattform-Sicherheit:** Sicherstellung der Sicherheit der Betriebssysteme, der Virtualisierungsplattformen und der zugrundeliegenden Software, auf denen die Kundensysteme laufen. Dies umfasst Patch-Management und Konfigurationshärtung der Infrastruktur.
- **Basisleistungen des Cloud-Anbieters:** Bereitstellung grundlegender Sicherheitsfunktionen wie Netzwerktrennung, Basis-Firewalls, Intrusion Detection Systems (IDS) und DDoS-Schutzmechanismen für die Plattform.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Verantwortung des Unternehmens

Das Unternehmen hingegen ist für die Sicherheit "in" der Cloud verantwortlich, also für die Daten, Anwendungen und Konfigurationen, die er in der Cloud betreibt. Diese Verantwortung umfasst:

- **Daten:** Schutz der eigenen Daten durch adäquate Verschlüsselung (im Ruhezustand und während der Übertragung), Implementierung strenger Zugriffskontrollen und Sicherstellung der Datenresidenz und Compliance-Anforderungen.

- **Anwendungen:** Absicherung der eingesetzten Anwendungen durch regelmäßiges Patch-Management, sichere Konfiguration (z. B. Entfernen von Standardpasswörtern), Absicherung von APIs und Durchführung von Sicherheitstests.

- **Zugriffe:** Management von Identitäten und Benutzerrechten (Identity and Access Management – IAM), Implementierung von Multi-Faktor-Authentifizierung (MFA) und Least Privilege Prinzipien, um sicherzustellen, dass nur autorisierte Benutzer auf die notwendigen Ressourcen zugreifen können.

- **Konfiguration:** Verantwortung für die sichere Einrichtung und Konfiguration der Cloud-Ressourcen, einschließlich Netzwerksegmentierung, Firewall-Regeln auf Anwendungsebene und Speicherkonfigurationen. Fehlkonfigurationen sind eine der häufigsten Ursachen für Cloud-Sicherheitsvorfälle.

Die Realität zeigt, dass viele Sicherheitslücken in Cloud-Umgebungen nicht durch grundlegende Schwächen der Cloud selbst entstehen, sondern durch Fehler und Versäumnisse des Unternehmens.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Dazu gehören häufig Fehlkonfigurationen von Cloud-Diensten, unzureichende Zugriffskontrollen oder das Fehlen moderner Schutzmechanismen, die über die Basisleistungen des Cloud-Anbieters hinausgehen. Dies betrifft insbesondere den Schutz auf mobilen Geräten, in Browsern oder bei der E-Mail-Kommunikation, die oft außerhalb des direkten Kontrollbereichs der Cloud-Infrastruktur liegen.

5. PHISHING ALS REALE GEFAHR - TYPISCHE SZENARIEN IN DEN KLEINEN UND MITTLEREN UNTERNEHMEN

Phishing stellt nach wie vor eine der größten und am weitesten verbreiteten Bedrohungen für kleine und mittlere Unternehmen (KMU) dar. Es handelt sich hierbei um den systematischen Versuch von Cyberkriminellen, über gefälschte Nachrichten – sei es per E-Mail, SMS, Messenger-Diensten oder sozialen Medien – an vertrauliche Informationen wie Zugangsdaten, Finanzdaten oder persönliche Identitäten zu gelangen. Die besondere Gemeinheit von Phishing-Angriffen liegt in ihrer oft täuschend echten Aufmachung und der geschickten Ausnutzung bestehender Vertrauensverhältnisse, sowohl innerhalb des Unternehmens als auch zu externen Geschäftspartnern.
In Gesprächen mit KMU-Verantwortlichen und bei Analysen von Sicherheitsvorfällen zeigt sich immer wieder, dass Phishing-Angriffe keine isolierten Einzelfälle sind, sondern zum bedauerlichen Alltag vieler Unternehmen gehören. Sie treten dort besonders erfolgreich auf, wo es an technischen Schutzmaßnahmen wie E-Mail-Filtern oder Link-Analyse-Tools mangelt und wo Mitarbeitende nicht ausreichend im Erkennen von Phishing-Versuchen geschult wurden.

Typische Phishing-Szenarien, die in KMU verbreitet sind, umfassen:

Finanz-Phishing (CEO-Fraud / Whaling)

Dieses Szenario ist besonders schädlich und zielt oft auf die oberste Managementebene oder die Finanzabteilung ab. Der Finanzverantwortliche erhält eine E-Mail, die scheinbar vom Geschäftsführer oder einer anderen hohen Führungskraft stammt.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Die Nachricht ist glaubwürdig formuliert, oft in ausgezeichnetem Deutsch und mit einer täuschend echten Signatur versehen. Die E-Mail enthält eine dringende Anweisung, eine hohe Geldsumme an einen neuen „Lieferanten“ oder „Geschäftspartner“ zu überweisen, oft unter dem Vorwand einer geheimen Akquisition, eines wichtigen Projekts oder einer einmaligen Gelegenheit. In Wirklichkeit ist der vermeintliche Empfänger ein Konto der Kriminellen, und das Geld ist unwiederbringlich verloren.

Kontodaten-Phishing (Credential Harvesting)

Mitarbeitende erhalten eine E-Mail oder SMS, die angeblich von ihrer Bank, einem bekannten Unternehmen (z. B. Microsoft, PayPal, Amazon) oder einem internen IT-Team stammt. Die Nachricht warnt vor verdächtigen Aktivitäten auf ihrem Konto, einer notwendigen Datenaktualisierung oder einer angeblichen Sperrung des Zugangs. Um „das Konto zu sichern“ oder den Dienst wieder nutzen zu können, werden sie aufgefordert, auf einen Link zu klicken und ihre Zugangsdaten auf einer gefälschten Website einzugeben, die der Originalseite zum Verwechseln ähnlichsieht. Diese erbeuteten Zugangsdaten werden dann für weitere Angriffe genutzt.

Rechnungs-Phishing (Malware-as-a-Service oder BEC)

Eine E-Mail mit einer täuschend echten Rechnung eines bekannten Dienstleisters (z. B. Telekomunikationsunternehmen, Energieversorger, Paketdienst) wird versendet. Die Nachricht enthält eine Zahlungsaufforderung und ist oft mit einem PDF-Anhang oder einem Link versehen. Der Anhang oder der Link laden entweder direkt Schadsoftware (z. B. Erbotet, Trickbot) auf das IT-System des Opfers, die dann weitere Malware nachlädt (z. B. Ransomware), oder sie führen zu einer gefälschten Zahlungsaufforderung, die das Geld auf ein Konto der Angreifer umleitet (Business E-Mail Compromise – BEC).

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Spear-Phishing (Gezielte Angriffe)

Im Gegensatz zu breit gestreuten Kampagnen zielt Spear-Phishing auf einzelne Mitarbeitende oder kleine Gruppen innerhalb des Unternehmens ab, z. B. aus der Buchhaltung, dem Einkauf oder dem Personalwesen. Die Angreifer investieren Zeit in die Recherche und nutzen öffentlich verfügbare Informationen (z. B. aus LinkedIn, Unternehmenswebseiten, sozialen Medien), um hochgradig personalisierte und glaubwürdige Anfragen zu formulieren. Sie kennen die Namen von Vorgesetzten, Projekten oder Geschäftspartnern und können so das Vertrauen des Opfers leicht gewinnen.

QR-Phishing (Quishing)

Dies ist eine neuere Variante des Phishings, bei der gefälschte QR-Codes eingesetzt werden. Diese QR-Codes können auf physischen Flyern, in E-Mails, auf Webseiten oder sogar in legitimen Dokumenten platziert werden. Scannt das Opfer den QR-Code mit seinem Smartphone, wird es nicht auf die erwartete, legitime Seite weitergeleitet, sondern auf eine präparierte Webseite. Diese Seite kann entweder direkt vertrauliche Daten abgreifen oder unbemerkt Malware auf das Gerät nachladen, was eine erhebliche Bedrohung darstellt, da QR-Codes oft als vertrauenswürdig wahrgenommen werden.

Was all diese Cyberangriffe gemeinsam haben, ist ein entscheidender Aspekt: Sie zielen nicht primär auf technische Schwachstellen ab, obwohl diese oft ausgenutzt werden, sondern auf den Menschen. Die Angreifer nutzen psychologische Faktoren wie Vertrauen, Neugier, Angst oder die Dringlichkeit, um Mitarbeitende zur Preisgabe von Informationen oder zum Klick auf schädliche Links zu bewegen. Und genau das macht sie so gefährlich. Ohne adäquate technische Unterstützung (z. B. intelligente Link-Analyse, Echtzeit-Erkennung von Phishing-Versuchen, Sandboxing von verdächtigen Anhängen) und vor allem ohne umfassende Schulung der Mitarbeitenden sind viele KMU diesen raffinierten Bedrohungen schutzlos ausgeliefert.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Die Phishing-Angriffe sind inzwischen noch gezielter, raffinierter und oft speziell auf die vermeintlichen Schwächen von KMU zugeschnitten, die oft nicht über die Ressourcen großer Unternehmen für Cybersicherheit-Schulungen verfügen.

6. EMPFOHLENE CYBERSICHERHEITSLÖSUNGEN FÜR KMU - INTEGRIERTE CYBERSICHERHEITSPLATTFORM STATT EINZELBAUSTEINE

Viele kleine und mittelständische Unternehmen setzen aus historisch gewachsenen Gründen oder aus Kostengründen immer noch auf eine Sammlung isolierter Einzellösungen für ihre Cybersicherheit. Dies sind typischerweise Antivirenprogramme auf den Endgeräten, dedizierte VPN-Zugänge für den Remote-Zugriff oder E-Mail-Gateways, die den E-Mail-Verkehr filtern. Diese punktuellen Schutzmaßnahmen, die oft von verschiedenen Anbietern stammen und nicht miteinander kommunizieren, bieten jedoch nur einen fragmentierten und ineffizienten Schutz. Angesichts der heutigen, komplexen und sich rasant entwickelnden Bedrohungslandschaft, die von Ransomware über hochintelligente Phishing-Kampagnen bis hin zu Zero-Day-Exploits reicht, genügt dieser Ansatz bei Weitem nicht mehr, um ein Unternehmen adäquat zu schützen.

Moderne Cybersicherheit für KMU muss in ihrer Konzeption grundlegend anders sein. Sie muss integriert, automatisiert und zentral steuerbar sein. Eine Plattformlösung ist hier der Schlüssel. Sie hat das Potenzial, die notwendige Sichtbarkeit, Kontrolle und den umfassenden Schutz zusammenzuführen, ohne die Komplexität zu erhöhen, die oft mit der Verwaltung zahlreicher einzelner Cybersicherheits-Silos einhergeht.

Eine solche Plattform ermöglicht einen holistischen Blick auf die Sicherheitslage und eine koordinierte Reaktion auf Bedrohungen.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Zentrale Cybersicherheitsplattform – Ganzheitlich verwalten statt verteilt kämpfen

Eine moderne Cybersicherheitsplattform dient als das Herzstück der Sicherheitsstrategie. Sie bietet eine zentrale “Single Pane of Glass“ Benutzeroberfläche, über die alle Sicherheitsmodule und -funktionen verwaltet und überwacht werden können.

Dies umfasst den Schutz von Endgeräten, mobilen Geräten, E-Mail-Verkehr, Web-Zugriffen, Cloud-Umgebungen, Benutzerzugriffen, Sicherheitsrichtlinien und die Reaktion auf Sicherheitsvorfälle.

Das Policy-Based Management ermöglicht eine rollenbasierte Zugriffssteuerung (RBAC), was für ein Unternehmen mit mehreren Niederlassungen von Vorteil ist. Zudem unterstützen fortschrittliche Plattformen die automatische Geräteeinbindung (Zero Touch Provisioning), was die Verwaltung einer großen Anzahl von Endgeräten erheblich vereinfacht.

Ein entscheidender Vorteil ist die KI-gestützte Risikobewertung und Bedrohungskorrelation, die beispielsweise auf Frameworks wie MITRE ATT&CK basiert. Dies ermöglicht es, komplexe Angriffsmuster zu erkennen, die über einzelne Indikatoren hinausgehen, und potenzielle Risiken proaktiv zu identifizieren und zu priorisieren.

Darüber hinaus bieten moderne Plattformen offene API-Schnittstellen für die Integration mit anderen IT-Systemen wie Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR) und Mobile Device Management (MDM) für eine nahtlose Automatisierung und ein umfassendes Sicherheitsmanagement.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Endgeräteschutz (EDR/XDR) – Phishing und Malware stoppen, bevor Schaden entsteht

Der Endgeräteschutz hat sich über traditionelles Antivirus hinausentwickelt. Moderne Lösungen umfassen Advanced Anti-Malware mit Verhaltensanalyse (Behavioral Analysis) und Heuristik, die nicht nur bekannte Signaturen, sondern auch verdächtiges Verhalten und unbekannte Bedrohungen erkennen. Funktionen wie Link-Rewrite (Umschreibung von Links zur Überprüfung), Attachment-Sandboxing (Ausführung verdächtiger Anhänge in einer isolierten Umgebung) und Domain-Spoofing-Erkennung (Identifizierung gefälschter Absenderadressen) verhindern, dass schädliche Inhalte überhaupt das Postfach erreichen.

Zusätzlich werden Threat Emulation & Extraction sowie Ransomware-Rollback-Funktionen integriert, die es ermöglichen, den Zustand eines IT-Systems vor einem Ransomware-Angriff wiederherzustellen. Die Erkennung von Skript- und dateilosen Angriffen, PowerShell-Monitoring und Lateral Movement Detection (Erkennung von Seitwärtsbewegungen im Netzwerk) sind essenziell, um fortgeschrittene, schwer zu erkennende Angriffe zu identifizieren.

Application Control und Device Control (für USB, WLAN, Bluetooth) ermöglichen eine feingranulare Steuerung, welche Anwendungen ausgeführt oder welche Geräte angeschlossen werden dürfen. Die Integration in SIEM/XDR/SOAR-Lösungen gewährleisten, dass Endpunkt-Telemetriedaten für eine umfassende Sicherheitsanalyse zur Verfügung stehen.

Mobile Security – App-Kontrolle, Netzwerk- und Geräteschutz in Echtzeit

Mobile Geräte sind zu einem integralen Bestandteil der Arbeitswelt geworden, stellen aber auch eine erhebliche Angriffsfläche dar. Mobile Security-Lösungen sollten daher folgende Funktionen beinhalten:

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

- App Control & Signaturprüfung, um sicherzustellen, dass nur autorisierte und sichere Apps installiert werden können, und blockieren Installationen bei fehlenden Zertifikaten. Jailbreak-/Root-Erkennung und Emulator Detection identifizieren manipulierte oder simulierte Geräte.
- Geofencing und kontextbasierte Zugriffsregeln (basierend auf Zeit, Ort, WLAN) ermöglichen eine dynamische Anpassung der Cybersicherheitsrichtlinien.
- VPN-Erzwingung (Split/Full Tunnel) und verschlüsselte Datenverbindungen gewährleisten sichere Kommunikation.
- Zero-Phishing für mobile Browser und Messenger (SMS, WhatsApp etc.) schützt vor Phishing-Angriffen, die speziell auf mobile Nutzer abzielen.
- Die Konnektivität zu MDM-Lösungen wie Microsoft Intune oder VMware Workspace ONE ermöglicht eine zentrale Verwaltung mobiler Geräte und ihrer Sicherheitskonfigurationen.

E-Mail Security - Idealerweise mit integriertem Schutz vor Datenverlust (DLP)

E-Mail ist nach wie vor der primäre Vektor für Cyberangriffe. Eine effektive E-Mail Security-Lösung ist daher unerlässlich. Insbesondere für KMU ist eine Lösung mit integriertem Schutz vor Datenverlust (Data Loss Prevention – DLP) von großem Vorteil.

Diese Lösungen verhindern nicht nur, dass schädliche Inhalte wie Malware, Viren und Phishing-Mails in die Posteingänge gelangen, sondern bieten auch effektiven Schutz vor Datenabfluss (DLP) in E-Mails, Anhängen und über Cloud-Kollaborationsdienste wie Microsoft 365 oder Google Workspace.

Dies minimiert das Risiko von Cyberangriffen, schützt vertrauliche Informationen und trägt zur Aufrechterhaltung der Geschäftskontinuität bei.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Die automatische Erkennung und Blockierung sensibler Inhalte (z. B. personenbezogene Daten, Finanzdaten, Kundendaten, geistiges Eigentum) ist eine Kernfunktion, die hilft, Compliance-Anforderungen zu erfüllen und unbeabsichtigten oder böswilligen Datenabfluss zu verhindern.

Der Vorteil für KMU liegt auch in der schnellen Bereitstellung ohne großen Aufwand, da diese Lösungen oft Cloud-basiert und vorkonfiguriert sind, was sie ideal für Unternehmen ohne eigene, große Cybersicherheit-Teams macht. Eine solche Lösung fungiert als All-in-One-Lösung, die Phishing-, Malware- und Datenabfluss-Schutz aus einer Hand bietet. Sie vereint leistungsstarke Cybersicherheit mit einfacher Handhabung für zuverlässigen Datenschutz und Compliance bei voller Produktivität.

Browser Security – Der neue Perimeter

Die moderne Arbeitswelt hat sich zunehmend in den Webbrowser verlagert. Vom Zugriff auf SaaS-Anwendungen über die Nutzung von generativen KI-Lösungen bis hin zur Arbeit auf nicht verwalteten Geräten – der Browser ist zum primären Arbeitswerkzeug geworden. Legacy-Sicherheitskontrollen sind für diese neue Realität oft nicht ausgelegt.

Das Ergebnis ist eine neue Angriffsfläche, die durch herkömmliche Firewalls oder Antivirenprogramme nicht ausreichend geschützt wird. Hier kommen Secure Enterprise Browser und AI Usage Control ins Spiel. Diese spezialisierten Browser sind darauf ausgelegt, die Cybersicherheit direkt am Punkt der Interaktion zu gewährleisten. Sie können bösartige Websites isolieren, sensible Daten vor unbeabsichtigter Offenlegung schützen und die Nutzung von KI-Tools überwachen und kontrollieren, um Compliance und Datensicherheit zu gewährleisten.

Die Anerkennung der Notwendigkeit dieser Lösungen ist ein entscheidender Fortschritt in der Cybersicherheit, da sie den Schutz dahin verlagern, wo die eigentliche Arbeit stattfindet, und die größten Risiken entstehen.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Zugriffssicherheit – Kontextbasiert statt implizites Vertrauen

Traditionelle VPNs gewähren oft einen breiten Zugang zum Netzwerk. Moderne Zugriffssicherheit basiert auf Zero Trust Network Access (ZTNA)-Prinzipien: Es wird keinem Benutzer oder Gerät standardmäßig vertraut, selbst wenn sie sich bereits im Netzwerk befinden. Der Zugriff wird nur auf autorisierte Ressourcen gewährt – und das nur unter Berücksichtigung des Kontexts, der Gerät, Nutzerrolle, Standort, Uhrzeit und Abteilung umfasst.

Schlüsseltechnologien sind Multi-Factor Authentication (MFA) und Single Sign-On (SSO) via SAML/OIDC, die die Authentifizierung stärken und die Benutzerfreundlichkeit erhöhen. Just-in-Time Access gewährt Berechtigungen nur für einen begrenzten Zeitraum, und der Device Posture Check stellt sicher, dass ein Gerät den Cybersicherheitsrichtlinien entspricht, bevor es Zugriff erhält. Das Least Privilege Access-Prinzip minimiert die Rechte eines Benutzers auf das absolut Notwendige. Granulare Zugriffsrichtlinien mit adaptiver Authentifizierung passen die Cybersicherheitsanforderungen dynamisch an das Risiko an. Revisionssichere Logging-Funktionen mit Zeitstempeln sind entscheidend für die Nachvollziehbarkeit und forensische Analysen.

Cloud Access Security Broker (CASB) – Transparenz und Kontrolle über Cloud-Anwendungen

Angesichts der zunehmenden Nutzung von Cloud-Diensten sind Cloud Access Security Broker (CASB)-Lösungen unverzichtbar. Ein CASB-Modul bietet sowohl Inline- als auch API-basierte Kontrolle. Es ermöglicht die Shadow-IT-Erkennung, um unautorisierte Cloud-Anwendungen zu identifizieren, und die SaaS-Kontrolle, um die Nutzung genehmigter Dienste zu überwachen.

Integrierte Data Lost Preventions (DLP)-Funktionen sind entscheidend, um den Abfluss sensibler Daten zu verhindern. Sie nutzen Regex, Templates und automatische Klassifizierung, um Daten wie Kreditkartennummern oder Sozialversicherungsnummern zu identifizieren und zu schützen.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Weitere Schutzmechanismen umfassen Tokenisierung, Verschlüsselung und Watermarking bei Uploads, um Daten auch in der Cloud zu schützen.

Anomalieerkennung (z. B. Massen-Downloads, Geosprünge) hilft, verdächtige Verhaltensweisen zu identifizieren. API-basierte Malware Detection, File Hashing und Cloud Sandbox ermöglichen die Analyse von Dateien und Inhalten in der Cloud auf Malware. Software-as-a-Service (SaaS) Visibility für gängige Dienste wie Office 365, Salesforce, Dropbox etc. und Cloud-to-Cloud Traffic Monitoring bieten einen umfassenden Überblick über den Datenfluss in der Cloud.

Firewall & SD-WAN (optional) – Performance und Cybersicherheit an jedem Standort

Für Unternehmen mit komplexeren Netzwerkanforderungen oder mehreren Standorten sind Firewall- und SD-WAN-Funktionalitäten eine wertvolle Ergänzung. Eine Cloud-delivered Next-Generation Firewall (NGFW) bietet fortschrittliche Filterung, einschließlich TLS-Inspection (Entschlüsselung und Überprüfung von verschlüsseltem Verkehr) und Application Awareness (Erkennung und Kontrolle von Anwendungen).

SD-WAN (Software-Defined Wide Area Network)-Funktionalität optimiert die Netzwerkleistung durch intelligente Pfadauswahl (Path Selection), Quality of Service (QoS) und Load Balancing (Lastverteilung). Dies ermöglicht eine effiziente Nutzung von Bandbreiten und eine verbesserte Anwendungsperformance.

Die zentrale Verwaltung von Netzwerk-Policies und Optimierungen vereinfachen die Konfiguration und Durchsetzung von Cybericherheitsregeln. Dynamische VPNs (Site-to-Site, Site-to-Cloud) gewährleisten sichere Verbindungen zwischen Standorten und zur Cloud. Funktionen wie GeoIP-Filterung (Blockieren von Verkehr aus bestimmten Ländern), URL-Kategorisierung und zentralisiertes Logging bieten umfassende Kontrolle und Transparenz über den Netzwerkverkehr.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Proaktive Datensicherheit - Verwaltung der Datensicherheitslage und Einhaltung von Compliance-Vorschriften

Ein weiterer entscheidender Baustein für eine moderne und proaktive Datensicherheitsstrategie ist der Einsatz der Data Security Posture Management (DSPM)-Lösung, die eine ganzheitliche Sicht auf die Datenlandschaft bietet und es Unternehmen ermöglicht, die Datenrisiken proaktiv zu priorisieren und zu beheben.

Hier sind einige der wichtigsten Funktion der Data Security Posture Management (DSPM)-Lösung:

- Lokalisierung sensibler Daten: DSPM-Lösung identifiziert und klassifiziert sensible Daten an verschiedenen Speicherorten, darunter Cloud-Systeme (SaaS, PaaS, IaaS), Fileserver, Datenbanken sowie Anwendungen, die von Mitarbeitenden ohne offizielle Freigabe nicht genutzt werden können.
- Überprüfung von Zugriffsrechten: DSPM-Lösung analysiert Zugriffsrechte und -muster, um zu überprüfen, wer auf welche Daten zugreifen kann. Es hilft dabei, übermäßige Berechtigungen zu identifizieren und sicherzustellen, dass der Zugriff auf sensible Daten dem Prinzip der geringsten Privilegien (Least Privilege) entspricht und wirklich notwendig ist.
- Empfehlungen zur Optimierung der Datensicherheit: Basierend auf der Analyse von Datenstandorten und Zugriffen liefert DSPM automatisierte Empfehlungen zur Verbesserung der Datensicherheit, zur Schließung von Dantesicherheitslücken und zur Einhaltung von Compliance-Vorgaben.

Durch die Implementierung der DSPM-Lösung wird aus einer reaktiven Verteidigung, die nur auf Angriffe reagiert, eine datenzentrierte, proaktive und lernfähige Cybersicherheitsstrategie. Der Fokus verlagert sich von der Perimeter-Sicherheit auf den Schutz der Daten selbst, was in einer Welt verteilter Daten und Cloud-Anwendungen unerlässlich ist.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Einsatz der KI-gestützten Cybersicherheitslösungen für bessere Cybersicherheit

Der Einsatz von Künstlicher Intelligenz (KI) revolutioniert die Cybersicherheit, insbesondere für KMU. KI-gestützte Cybersicherheitslösungen sind in der Lage, riesige Datenmengen zu analysieren und komplexe Muster zu erkennen, die für menschliche Analysten nur schwer zu identifizieren wären. Durch den Einsatz von KI lassen sich Bedrohungen nicht nur signifikant schneller erkennen, sondern auch automatisch priorisieren und mit den passenden Gegenmaßnahmen versehen. Dies entlastet die IT-Abteilung erheblich, indem sie sich auf die wichtigsten Alarme konzentrieren kann und Routinetätigkeiten automatisiert werden. Besonders in kleineren Unternehmen mit begrenzten personellen Ressourcen kann KI die IT unterstützen, anstatt sie zu überlasten, und so die Effektivität der Sicherheitsmaßnahmen erheblich steigern.

7. SPEZIFISCHE CYBERSICHERHEITSMASSNAHMEN FÜR KI UND KI-GESTÜTZTE LÖSUNGEN

Angesichts der zunehmenden Nutzung von KI sind spezifische Cybersicherheitsmaßnahmen unerlässlich:

Schutz auf Modellebene

Für produktive KI-Pipelines, in denen Modelle aus Kundendaten lernen oder automatisierte Entscheidungen treffen, werden folgende Maßnahmen empfohlen:

- Validierung und Bereinigung von Trainingsdaten.
- Erkennung von unerwünschten Eingaben während der Inferenzphase oder Überwachung des Modellverhaltens (Drifterkennung, Anomalien).
- Ratenbegrenzung für den API-Zugriff auf ML-Modelle oder Einsatz von Modell-Wasserzeichen und Zugriffskontrollen.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Der Datentransparenz mit Data Security Posture Management (DSPM): DSPM-Lösungen sind entscheidend für die Identifizierung und Klassifizierung sensibler und vertraulicher Daten in einem Unternehmen. Sie helfen, Risiken frühzeitig zu adressieren, z. B. die Weitergabe sensibler Daten an Unbefugte zu verhindern und Datenverluste zu vermeiden, bevor Schutzmaßnahmen überhaupt greifen. DSPM bietet kontinuierliche Transparenz über sensible Daten und deren Schutzbedarf. Unternehmen können erkennen, wo sich sensible Daten befinden (Cloud, Dateisystem, Shadow-Tools), kontrollieren, wer Zugriff hat (und ob dieser wirklich notwendig ist) und erhalten automatisierte Empfehlungen zur proaktiven Verbesserung der Datensicherheit.

Schutz sensibler Datenbewegungen mit Data Loss Prevention (DLP): Zusätzlich zu DSPM ist die Implementierung einer DLP-Lösung unerlässlich, um sensible Daten umfassend vor unbefugtem Zugriff, Diebstahl oder Verlust zu schützen. DLP hilft, Datenschutzverletzungen zu verhindern, die Einhaltung von Vorschriften zu gewährleisten und finanzielle Schäden sowie Reputationsschäden zu minimieren. Ein umfassender DLP-Ansatz kombiniert technische Lösungen, Richtlinien und die Sensibilisierung der Mitarbeiter.

Schutz generativer KI und KI-gestützter Lösungen durch Browsersicherheit

Da Mitarbeiter in der Regel über Webbrowser auf generative KI und KI-gestützte Software-as-a-Service (SaaS)-Lösungen zugreifen, besteht für Unternehmen das Risiko eines Datenverlusts durch die unkontrollierte Übertragung vertraulicher Unternehmensdaten (wie Kundendaten, Quellcode oder Finanzinformationen) an externe KI-Plattformen. Browser-Sicherheitslösungen können Unternehmen dabei unterstützen, integrierte Cybersicherheitsregeln zu nutzen und eigene Richtlinien zu erstellen, um die Cybersicherheits-Governance durchzusetzen, Benutzeraktivitäten mit generativen KI-Lösungen einzuschränken, Datenlecks zu verhindern oder unbefugte KI und KI-gestützte SaaS-Lösungen zu blockieren.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Moderne Browser-Sicherheitsfunktionen umfassen die Erkennung und Blockierung sensibler Daten direkt im Browser, kontextabhängige Richtlinien für die Nutzung generativer KI (z. B. Schreibschutz, Zwischenablage-Blocker), die Protokollierung der Nutzung von Web-KI-Diensten und die Integration in bestehende DLP- oder Cloud Access Security Broker (CASB)-Systeme. Diese Funktionen ermöglichen den sicheren Einsatz generativer KI, auch in Bring-Your-Own-Device-KI-Szenarien (BYOAI) oder offenen SaaS-Umgebungen.

8. DIE EINHEITLICHE CYBERSICHERHEITSPLATTFORM - GRUNDLAGE FÜR CYBERSICHERHEIT-VERSICHERUNGEN

Die Implementierung einer modernen und einheitlichen Cybersicherheitsplattform, wie sie von AQ SECURE empfohlen wird, bietet nicht nur direkten Schutz vor Cyberangriffen, sondern auch einen entscheidenden Vorteil: die Nachweisbarkeit und Transparenz der Cybersicherheitsmaßnahmen. Dies ist von fundamentaler Bedeutung, wenn es um den Abschluss und die Bedingungen von Cybersicherheit-Versicherungen geht.

Versicherer verlangen zunehmend detaillierte Nachweise über die implementierten Cybersicherheitsvorkehrungen, bevor sie eine Cyberversicherung anbieten oder ihre Prämien festlegen. Eine umfassende Plattform erleichtert diesen Prozess erheblich durch:

- **Transparenz und Monitoring:** Die Plattform liefert nachvollziehbare Logs, Ereignisketten und detaillierte Aufzeichnungen über Reaktionen auf Cybersicherheitsvorfälle. Diese Telemetriedaten sind für Versicherer von großem Wert, um das Risikoprofil eines Unternehmens objektiv einschätzen zu können.

- **Prozesse und Richtlinien:** Eine Plattform hilft bei der Durchsetzung und Dokumentation von klar definierten Zugriffsregeln, einer stringenten Benutzerverwaltung und etablierten Eskalationswegen im Falle eines Cybersicherheitsvorfalls. Dies demonstriert dem Versicherer, dass das Unternehmen über eine organisatorische Struktur zur Risikosteuerung verfügt.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

- **Daten- und Zugriffsabsicherung:** Die durch die Plattform gewährleistete umfassende Absicherung von Daten und Zugriffen auf allen Ebenen bildet eine solide Grundlage für die Risikobewertung durch die Versicherer. Unternehmen, die nachweislich moderne Schutzmechanismen (wie Zero Trust, MFA, DLP) implementiert haben, werden tendenziell als weniger riskant eingestuft.

Eine solche Cybersicherheitsplattform schützt Unternehmen somit nicht nur proaktiv vor den direkten Folgen von Cyberangriffen. Sie schafft darüber hinaus die notwendige Grundlage für den Abschluss einer Cyberversicherung, indem sie die Compliance-Anforderungen erfüllt und die Risikobereitschaft des Unternehmens minimiert. Dies kann maßgeblich dazu beitragen, Unternehmen von erheblichen finanziellen Risiken abzusichern, die aus einem Cyberangriff entstehen könnten, wie zum Beispiel Betriebsunterbrechungen, Wiederherstellungskosten, Bußgelder oder Reputationsschäden.

9. FAZIT: CYBERSICHERHEITSPLATTFORM MIT ALLEN ERFORDERLICHEN CYBERSICHERHEITSLÖSUNGEN FÜR KMU

Eine integrierte Cybersicherheitsplattform bietet KMU nicht nur einen umfassenden Schutz für Geräte, Nutzer und Daten, sondern auch die entscheidende Möglichkeit, ihr Geschäft flexibel und sicher zu entwickeln. Der modulare Aufbau ermöglicht es, die Lösung skalierbar an neue Standorte, wachsende Mitarbeiterzahlen oder sich ändernde Arbeitsmodelle anzupassen, ohne die Cybersicherheit zu beeinträchtigen. Die budgetgerechte Gestaltung durch modulare Auswahl und Priorisierung bedeutet, dass Unternehmen nur für die Funktionen bezahlen, die sie tatsächlich benötigen, und schrittweise erweitern können. Schließlich ist die Lösung zukunftssicher durch die konsequente Ausrichtung an SASE-Prinzipien und einer Zero-Trust-Basis, was sie widerstandsfähig gegenüber neuen Bedrohungen und Technologien macht. Cybersicherheit sollte niemals ein Hindernis sein, sondern ein Ermöglicher für Innovation und Wachstum.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

Genau das liefern moderne Plattformlösungen – intelligent kombiniert, passgenau umgesetzt und auf die spezifischen Anforderungen von KMU zugeschnitten.

Mit AQ SECURE: Cybersicherheit, die zu Ihrem Unternehmen passt

Wir von AQ SECURE verstehen die spezifischen Herausforderungen von KMU und begleiten Unternehmen pragmatisch, fokussiert und technologieoffen auf dem Weg zu einer sicheren IT-Landschaft. Unser Ansatz unterscheidet sich bewusst von der Implementierung isolierter Cybersicherheitslösungen und setzt stattdessen auf ein strukturiertes und kundenorientiertes Vorgehen:

- **Gemeinsame Planung:** Jeder erfolgreichen Cybersicherheitsstrategie geht eine detaillierte Analyse voraus. Wir beginnen damit, Ihre bestehende IT-Umgebung, die vorhandene Infrastruktur, identifizierte Schwachstellen und Ihre spezifischen Prioritäten umfassend zu analysieren. Dabei verzichten wir bewusst auf pauschale Umstellungen oder die Implementierung überflüssiger Maßnahmen. Unser Ziel ist es, ein klares Bild Ihrer Risikolandschaft zu gewinnen und zielgerichtete Empfehlungen zu entwickeln.

- **Passgenaue Umsetzung:** Basierend auf der Analyse erhalten Sie von uns genau die Cybersicherheitslösungen, die Sie wirklich benötigen – nicht mehr und nicht weniger. Dies gewährleistet eine effiziente Ressourcennutzung und vermeidet unnötige Komplexität oder Kosten, die oft mit überdimensionierten Cybersicherheitslösungen einhergehen.

- **SASE-Plattform mit integrierter Cybersicherheit:** Auf Wunsch stellen wir Ihnen eine erprobte SASE-Lösung eines spezialisierten Herstellers bereit, die sich in der Praxis bewährt hat. Dies umfasst eine Pilotierung in Ihrer Umgebung, um die Eignung und Funktionalität zu testen, sowie die spätere Skalierung der Lösung gemäß Ihren Wachstumsanforderungen. Wir arbeiten mit führenden Anbietern zusammen, um sicherzustellen, dass Sie Zugang zu den besten am Markt verfügbaren Technologien erhalten.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

- **Transparente Beratung:** Bei AQ SECURE legen wir großen Wert auf Transparenz. Wir bieten keine "Blackbox"-Lösungen. Sie behalten jederzeit die volle Kontrolle und den Überblick über Zugriffe, Datenflüsse und die angewandten Richtlinien. Unsere Beratung ist darauf ausgerichtet, Ihnen das Verständnis für die implementierten Maßnahmen zu vermitteln und Sie in die Lage zu versetzen, fundierte Entscheidungen zu treffen.

- **Optional mit SOC (Security Operations Center):** Für Unternehmen, die die Überwachung und Reaktion auf Cybersicherheitsvorfälle auslagern möchten, integrieren wir einen zuverlässigen SOC-Service. Ein SOC bietet 24/7-Überwachung, proaktive Bedrohungserkennung und schnelle Reaktion auf Incidents, was besonders für KMU ohne eigene dedizierte Cybersicherheitsteams eine erhebliche Entlastung darstellt und die Reaktionsfähigkeit immens verbessert.

AQ SECURE steht für lösungsorientierte Cybersicherheitskonzepte, die gezielte Optimierungen dort umsetzen, wo Verbesserungsbedarf besteht, ohne unnötige oder radikale Umstellungen vorzunehmen. Unser Fokus liegt auf effizienten Cybersicherheitsmaßnahmen, die einen spürbaren Mehrwert bieten. Grundlegende Neuerungen erfolgen nur dann, wenn sie nachweislich notwendig und sinnvoll sind, um Ihre Cybersicherheitslage signifikant zu verbessern.

Mehr als Technik: Sichtbarkeit, Kontrolle und Cybersicherheit mit Augenmaß

Cybersicherheit im modernen Sinne bedeutet weit mehr als nur das Absichern von Netzwerken, Geräten und Cloud-Anwendungen. Es geht darum, ein tiefgreifendes Verständnis für die eigene digitale Umgebung zu entwickeln und strategische Fragen beantworten zu können:

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

AQ SECURE

- **Welche Daten sind geschäftskritisch?**
  Die Identifizierung und Klassifizierung sensibler Daten ist der erste Schritt, um Schutzmaßnahmen priorisiert und gezielt anwenden zu können.

- **Wer darf worauf zugreifen – und wann?**
  Die präzise Verwaltung von Identitäten und Zugriffsberechtigungen (IAM) ist entscheidend, um unbefugten Zugang zu verhindern und das Prinzip der geringsten Rechte (Least Privilege) umzusetzen.

- **Wie erkenne ich Risiken frühzeitig – und reagiere automatisch?**
  Eine effektive Cybersicherheitsstrategie muss die Fähigkeit zur proaktiven Bedrohungserkennung und zur automatisierten Reaktion aufweisen, um Schäden zu minimieren und die Widerstandsfähigkeit zu erhöhen.

Mit der richtigen Cybersichereitsplattform und unserer Erfahrung als Partner bringt AQ SECURE Sichtbarkeit, Kontrolle und Cybersicherheit in Einklang.

Sie erhalten volle Transparenz über Ihre gesamte IT-Umgebung – von den Endpunkten bis zur Cloud und gleichzeitig die Flexibilität, Cybersicherheitsmaßnahmen dynamisch an neue Bedrohungen und sich ändernde Geschäftsanforderungen anzupassen.

Wir helfen Ihnen, die Cybersicherheitsverwaltung zu vereinfachen, routinemäßige Prozesse zu automatisieren und gezielt dort zu investieren, wo es wirklich zählt sowohl aus technischer als auch aus wirtschaftlicher Perspektive.

AQ SECURE steht für effektive Cybersicherheit, die wirkt und dabei Ihr Budget berücksichtigt.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de