QS solutions

White Paper

Security Assessment: nur die erste Station Ihrer Cyber Security

Bilden Sie den Status Ihrer Cyber Security mit regelmäßigen Bewertungen ab und entdecken Sie, wo die Schwachstellen und Risiken in Ihrer Organisation liegen.

Schützen Sie Ihre Organisation langfristig und effizient vor Cyberangriffen.

Inhalt

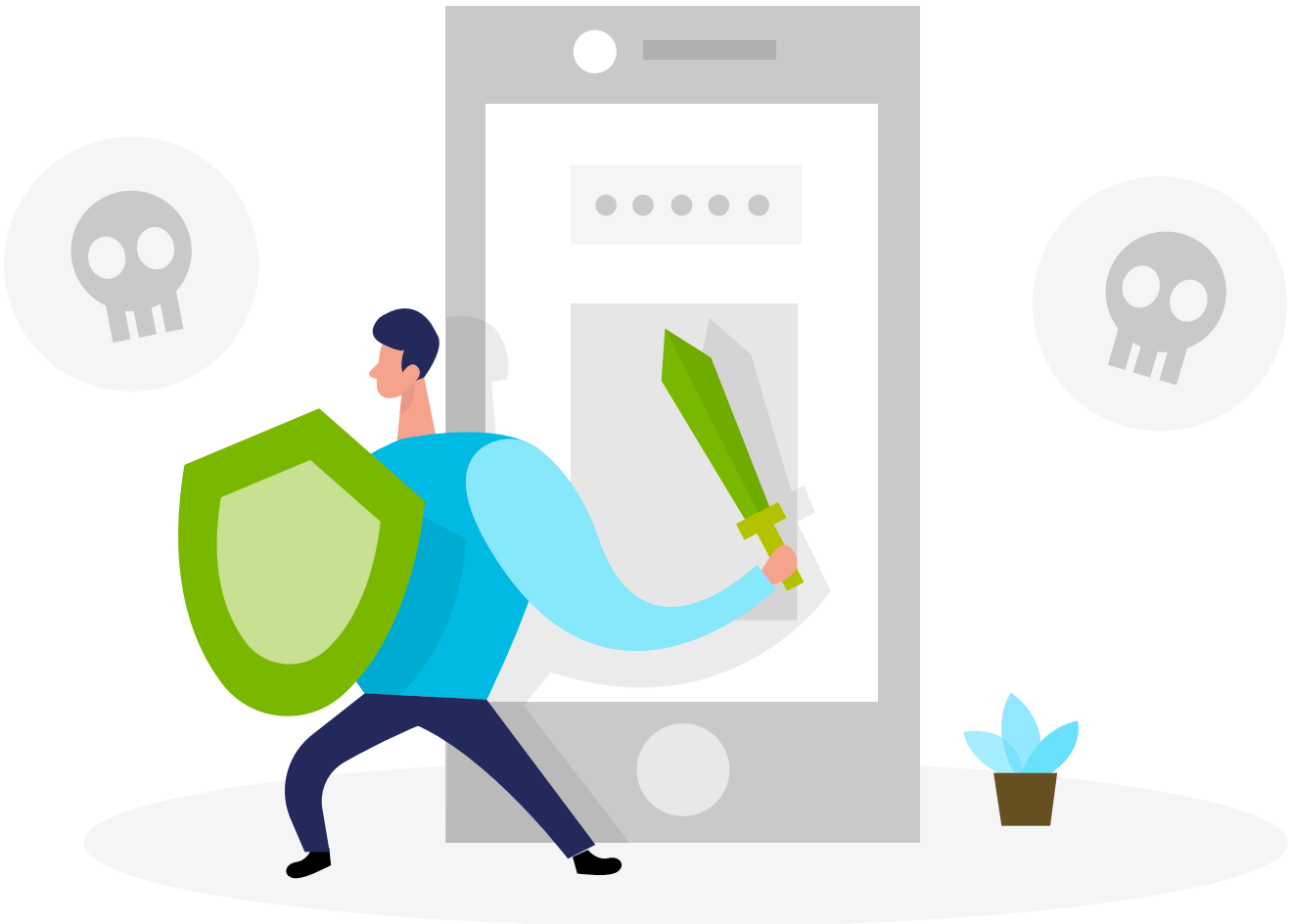
Die Cyber-Risiken der neuen Normalität

Die Corona-Pandemie hat die digitale Welt auf den Kopf gestellt. Während sich das Virus schnell auf der ganzen Welt ausbreitete, mussten genauso schnell neue Konzepte für die Zusammenarbeit geschaffen werden. Daraus entstand ein digitales Schlaraffenland für Cyberkriminelle, die nun versuchen überstürzt aufgesetzte IT-Infrastrukturen und unsichere Umgebungen zu attackieren. Die Arbeit von zu Hause aus wurde für Millionen von Menschen zur Norm, selbst in Branchen, in denen dies vor der Pandemie sicherlich nicht der Standard war. Eine dynamische Arbeitsweise gewann an Selbstverständlichkeit und machte die bestehenden Cyber-Risiken noch größer und sichtbarer. Mitarbeiter arbeiteten oft mit einer suboptimal gesicherten Infrastruktur und griffen auf private Geräte und moderne Apps zurück, um mit Kollegen und Kunden zu kommunizieren, oft ohne Absprache und Erlaubnis der IT-Abteilung.

In der Zwischenzeit wurden Hacker opportunistisch und klüger, raffinierter und organisierter. Und das belegen auch die Zahlen. Laut einem Bericht von Interpol 1) hat die Pandemie beispiellose Auswirkungen auf die globale Cyber-Bedrohungslandschaft und es ist wahrscheinlich, dass sie sich weiter verschlimmern wird. Cyberkriminelle entwickeln und führen ihre Angriffe mit alarmierender Geschwindigkeit aus. Sie nutzen die Angst und Unsicherheit, die durch die instabile soziale und wirtschaftliche Situation auf der ganzen Welt verursacht wurde. Gleichzeitig wächst das Risiko von Cyber-Einbrüchen und -Angriffen aufgrund der zunehmenden Abhängigkeit von Konnektivität und digitaler Infrastruktur.

Wie viel Technologie braucht Ihr Unternehmen, um am Laufen zu bleiben? Jede Anwendung und jedes Gerät ist ein Risiko. Und aufgrund der massiven Heimarbeit haben Sie viel weniger Kontrolle darüber, welche Anwendungen und Geräte Ihre Mitarbeiter verwenden. Es stellt sich also nicht mehr die Frage ob, sondern wann Ihre Organisation mit einer Sicherheitslücke konfrontiert wird.

1) Interpol – Cybercrime: COVID-19 Impact (August 2020)



Folgen von Datenschutzverletzungen

Wenn etwas schief geht, kann das enorme Folgen haben. Nicht nur finanziell – zum Beispiel Lösegeldzahlungen und die Kosten für Ausfallzeiten, Datenverlust und Wiederherstellung von Systemen – sondern auch mit Blick auf die Reputation Ihres Unternehmens und das Vertrauen der Kunden:

Datenschutzverletzungen treten immer häufiger auf und es wird darüber auch in den Medien ausführlich berichtet. Kunden müssen sich mehr denn je bewusst sein, dass Datensicherheit keine Selbstverständlichkeit ist. Sie berücksichtigen dies zunehmend bei der Auswahl eines Unternehmens oder einer Organisation. Laut Forschung 2) sind sogar 84 % der Kunden Unternehmen mit strenger Datensicherheit treuer.

Auch die EU erarbeitet nun Regelungen zur verbindlichen Cybersicherheit. Die neuen Regeln gelten nicht nur für lebensnotwenige Unternehmen und Institutionen wie Banken, Krankenhäuser, Gesundheitseinrichtungen und Versorgungsunternehmen. Auch andere Unternehmen mit einem Jahresumsatz von (mindestens) 10 Millionen Euro und fünfzig Mitarbeitern sind bald verpflichtet, ihre IT-Systeme auf Schwachstellen zu überprüfen, Risikoanalysen durchzuführen, ihre Sicherheit zu verbessern und am besten tägliche Backups zu machen.

Immer mehr Vorstände und Managementteams erkennen nun, dass Sicherheit nicht nur ein technologisches Thema ist. Es ist eine Aufgabe für die gesamte Organisation und erfordert Visionen von der Vorstandsetage. Cybersicherheit ist daher zu einem wichtigen Bestandteil der Organisationsstrategie geworden, obwohl dies immer noch regelmäßig vergessen wird.

2) ZDNet: Top 8 trends shaping digital transformation in 2021

Cyber-Resilienz ist eine ganzheitliche Strategie

Als Unternehmen geht es also darum, Cyber-Resilienz zu werden: Sie müssen in der Lage sein, Cyber-Angriffe zu überstehen, kritische Prozesse und Aktivitäten aufrechtzuerhalten und neue Technologien zu nutzen. Auch die ständig wechselnden Bedrohungen erfordern eine klare Agilität. Man muss in der Lage sein, mitzumachen, was passiert, aber mit einer klaren Vision. Und mit einem durchdachten, strategischen Ansatz zur Informationssicherheit mit ausgefeilten Prozessen, damit Sie Ihre kritischen Prozesse und Aktivitäten weiterhin schützen, immer wachsam bleiben und schnell und belastbar auf Vorfälle reagieren.

Und das alles, ohne die Produktivität der Organisation zu beeinträchtigen. Letzteres ist besonders wichtig, denn Ihre Mitarbeiter müssen natürlich weiterhin Zugriff auf die Anwendungen und Daten haben, mit denen sie ihre Arbeit erledigen können, egal ob im Büro, im Home-Office oder unterwegs. Das ist im Moment die Herausforderung für die Sicherheit mit höchster Priorität.

Ein guter Anfang...

Wo beginnt also Cyber-Resilienz? Und wie kommt man zu einer starken Sicherheitsstrategie? Tatsache ist, dass herkömmliche Datensicherheit nicht mehr ausreicht. Das Einrichten eines sicheren und konformen Netzwerks vor Ort für Ihre Organisation und der Versuch, alle Unternehmensressourcen dort unterzubringen, gehört nicht mehr in unsere Zeit. In diesem digitalen Zeitalter ist eine breitere, aber vor allem adaptive Strategie erforderlich. Eine, die sich an die zunehmende Komplexität und Dynamik unserer Arbeitsweise anpassen kann. Wer berücksichtigt, dass Mitarbeiter jederzeit, überall und von jedem Gerät aus arbeiten können müssen. Dazu müssen sie sich lediglich an ihrem digitalen Arbeitsplatz anmelden. Dies birgt neue Risiken und erfordert eine überarbeitete Cybersicherheitsstrategie.

Eine logische – und notwendige – erste Frage lautet: Wie geht Ihre Organisation derzeit mit digitalen Bedrohungen um? Wie ausgereift sind Ihre aktuellen Cyber-Security-Maßnahmen? Und können Sie bei Bedarf proaktiv handeln? Vor allem aber: Wo soll man bei der Überprüfung der Sicherheitsstrategie ansetzen? Wo liegen Schwachstellen und Risiken?

Für die meisten Unternehmen und Organisationen ist es einfach nicht machbar, mehrere große Veränderungen auf einmal zu realisieren. Klein anfangen ist daher die Devise. Ein phasenweises Vorgehen, bei dem Sie sich zunächst auf Bereiche konzentrieren, in denen die Cyber-Security noch nicht ausgereift ist. Diese Bereiche werden teilweise auf der Grundlage der verfügbaren Ressourcen und Prioritäten festgelegt. Welches Budget steht zur Verfügung? Was sind die unmittelbaren Geschäftsanforderungen? Mit anderen Worten: Was müssen Sie jetzt anpacken und was ist möglich?

Basismessung

Um die Sicherheitsstrategie effektiv in Angriff zu nehmen, ist es daher wichtig, den Ausgangspunkt zu bestimmen und eine Basismessung durchzuführen. Wie ausgereift ist Ihre Cybersicherheit jetzt? Welchen Umfang hat Ihre Informationssicherheit? Die folgenden Elemente geben einen starken Hinweis darauf:

- Wie stark ist die **Authentifizierung**? Verwenden Sie eine starke Multi-Faktor-Authentifizierung? Wie minimieren Sie das Risiko von identitätsbezogenen Sicherheitsverletzungen?

- Wie anpassungsfähig sind Ihre **Zugriffsrichtlinien**? Haben Sie klare Richtlinien für den akzeptablen Zugriff auf Ressourcen? Und wie setzen Sie diese durch?

- Arbeiten Sie bereits an **Mikrosegmentierung**? Inwieweit bewegt sich Ihr Unternehmen auf eine umfassende und verteilte Segmentierung mit softwaredefinierten Mikroperimetern zu?

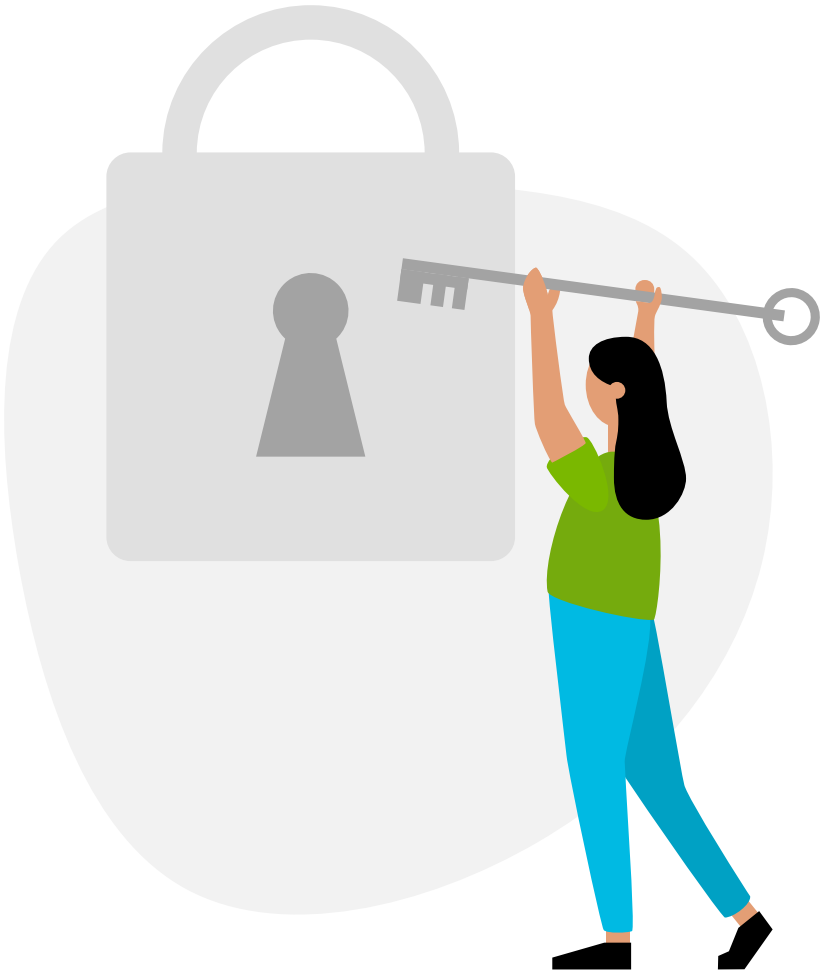
- Arbeiten Sie bereits mit **automatisierten Warnungen und Abhilfemaßnahmen**, um die durchschnittliche Zeit zwischen Angriff und Reaktion zu minimieren?

- Setzen Sie bereits **künstliche Intelligenz und Cloud-Intelligenz** ein, um Anomalien in Echtzeit zu erkennen und darauf zu reagieren?

- Inwieweit **klassifizieren und schützen** Sie Ihre Daten? Wie minimieren Sie, dass sensible Daten einer böswilligen oder versehentlichen Exfiltration, d. h. der unbefugten Freigabe von Daten aus Computersystemen, ausgesetzt sind?

Von hier aus können Sie dann auf die Cyber-Resilienz der Organisation aufbauen.

Um einen strukturierten und detaillierten Einblick in den Reifegrad Ihrer Cybersicherheit zu allen relevanten Elementen zu erhalten, empfehlen wir ein **cyber security assessment** bei QS solutions. Dieses untersucht Ihr gesamtes Unternehmensnetzwerk sowie Ihre Microsoft 365- und Azure-Umgebung auf mögliche Sicherheitslücken und verschafft Ihnen einen klaren Überblick über Schwachstellen und Risiken.



CSAT auf den Punkt gebracht

Unser Cyber Security Assessment Tool (CSAT) basiert auf dem CIS-Framework, einer weit verbreiteten Reihe von Best Practices, die für das strukturierte Management von Cyber-Risiken in Unternehmen und Organisationen entwickelt wurden. Es hilft Ihnen bei der Beantwortung kritischer Fragen zum Cybersicherheitsprogramm Ihres Unternehmens, z. B. dazu, welches Inventar geschützt werden soll und wo Sicherheitslücken bestehen.

Die Sicherheitsbewertung bietet die folgenden Funktionen:

- On premise – das Bewertungstool wird auf einem Server im Netzwerk installiert

- Endpoints – Durch eine Stichprobenprüfung werden die Laptops, Desktops und Server im Netzwerk überprüft

- Microsoft 365 – Kontrolle über alle genutzten (und gemeinsam genutzten) Dienste

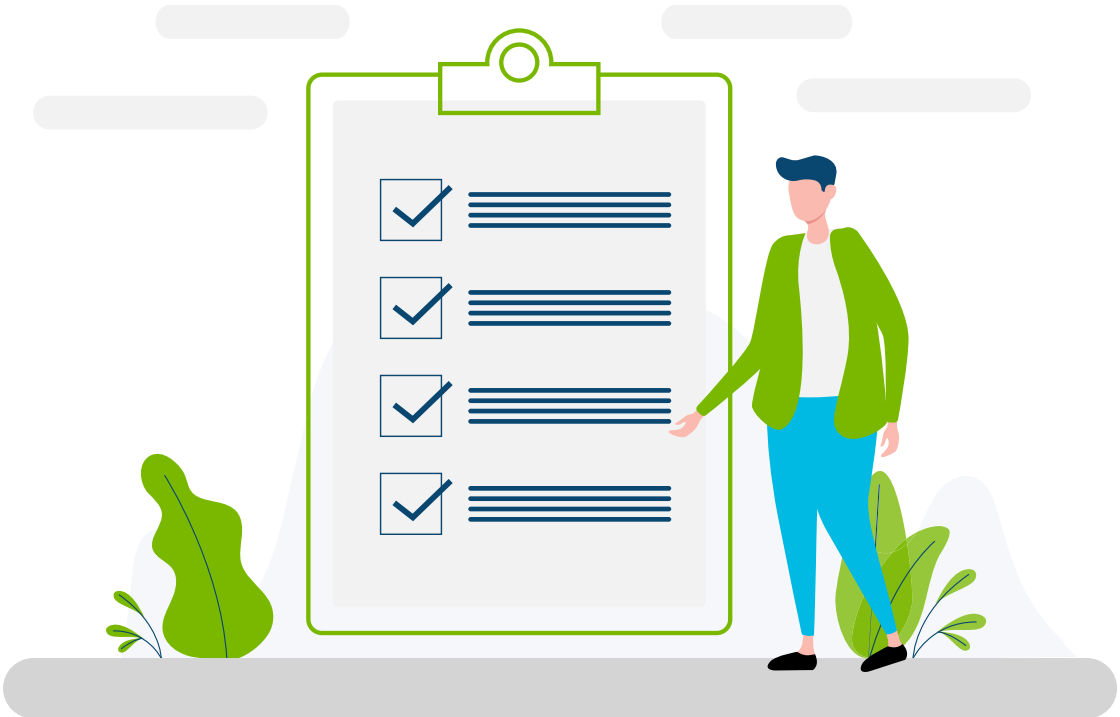
- Azure platform – Verstehen Sie die sichere Nutzung der Cloud-Plattform

- (Azure) Active Directory – Bewertung der gesamten (Azure) Active Directory Umgebung

- Umfrage – Einer unserer Sicherheitsberater fragt nach Sicherheitsprozessen und - verfahren

Im Rahmen der Sicherheitsbewertung prüfen wir unter anderem, ob Windows sicher konfiguriert ist und ob die richtigen Patches eingespielt wurden. Wir prüfen auch administrative Berechtigungen und externe Benutzer in Microsoft 365, Teams oder die freigegebenen Dokumente in SharePoint. Diese Erkenntnisse bestimmen den aktuellen Sicherheitsreifegrad der Organisation, auf dessen Grundlage konkrete Verbesserungsmaßnahmen vorgeschlagen werden können.

Die Bewertung fügt sich nahtlos in eine Zero-Trust-Richtlinie ein, die alle Mitarbeiter, Geräte und Anwendungen sichert, wo immer sie sich befinden, ohne die Produktivität zu beeinträchtigen. Wie eine solche „Zero Trust“-Policy umgesetzt wird, ist von Organisation zu Organisation unterschiedlich, aber die Grundlage ist dieselbe, nämlich die Sicherung von Unternehmensdaten und -anwendungen nach dem Prinzip „Nie vertrauen, immer prüfen“. Ausgehend von dieser Vision konzentrieren Sie sich auf die Sicherheit und Compliance von Unternehmenswerten, unabhängig von deren physischem Standort oder Platz im Netzwerk.



Gezielte Verbesserung

Dank der Sicherheitsbewertung erhalten Sie schnell einen Einblick in die Cyber-Risiken für Ihre Organisation und inwieweit die aktuellen Sicherheitsmaßnahmen ausreichend Schutz bieten. Es deckt potenzielle Schwachstellen und Risiken auf und ermöglicht es Ihnen, fundierte Entscheidungen über Prioritäten innerhalb Ihrer Cybersicherheit zu treffen: Wir werden zuerst unser Sicherheitsbudget dafür ausgeben.

Der CSAT bietet einen klaren Aktionsplan, um die Cybersicherheit Ihrer Organisation genau dort zu verbessern, wo sie benötigt wird. Und inklusive klarer technologischer und prozessualer Maßnahmen, damit Sie sofort loslegen und Ihre Ressourcen gezielt einsetzen können.

Mit einem Cybersicherheits-Assessment erhalten Sie Einblick in die Sicherheitsrisiken der Organisation und priorisieren schnell und effektiv die vorgeschlagenen Verbesserungsmaßnahmen auf der Grundlage von Fakten.

Bleiben Sie am Puls der Zeit

Nach der Umsetzung der Verbesserungsmaßnahmen ist es wichtig, anhand einer zweiten Bewertung zu messen, was sich im Vergleich zur Basismessung verbessert hat. Vergessen Sie nicht, das Führungsteam in die Präsentation der Ergebnisse einzubeziehen, damit auch dieses sich der reduzierten Risiken und der gestiegenen Cyber Security-Reife der Organisation bewusst ist.

Der nächste Schritt ist die Priorisierung, Ausarbeitung und Planung der folgenden Ziele. Cybersicherheit hat einfach keinen Anfangs- und Endpunkt. Es ist unmöglich, gleich beim ersten Mal alles richtig zu machen, daher ist es wichtig, darauf einen kontinuierlichen Fokus zu legen.

Stellen Sie eine kontinuierliche genaue Dokumentation von Status, Fortschritt und Verbesserungsmaßnahmen sicher. Dies ist nicht nur für den internen Gebrauch wertvoll, sondern auch im Hinblick auf die Einhaltung von Gesetzen und Vorschriften, beispielsweise zur DSGVO, unverzichtbar.

Die IT-Welt verändert sich in rasantem Tempo und damit auch die Cyberkriminellen. Digitale Bedrohungen entwickeln sich ständig weiter. Auch wenn eine einmalige Bewertung eine detaillierte Basismessung der aktuellen Cyber Security-Reife und potenzieller Schwachstellen und Risiken liefert, ist es entscheidend, am Puls der Zeit und jederzeit wachsam zu bleiben.

Lehnen Sie sich also nicht zurück, sondern evaluieren Sie weiterhin proaktiv den Sicherheitsstatus und berichten Sie über Fortschritte. Die **regelmäßige Wiederholung der Sicherheitsbewertung** ist ein wesentlicher Bestandteil einer gesunden Sicherheitsstrategie. Es vermittelt ein Bild über die Entwicklung der Cyber-Resilienz der Organisation als Ganzes und der verschiedenen Komponenten der Infrastruktur.

Auf diese Weise können Sie verschiedene Sicherheitsrisiken managen und neuen Formen der Cyberkriminalität einen Schritt voraus sein, ohne dass die Informationssicherheit die Produktivität beeinträchtigt.

Uber QS solutions

Bei QS solutions wissen wir, wie anfällig Organisationen sind. Und welche Folgen es haben kann, wenn eine Organisation den Reifegrad der Cybersicherheit nicht proaktiv verbessert. Wir beginnen mit unserem **Cyber Security Assessment Tool (CSAT),** um den Status der Sicherheit schnell und einfach zu visualisieren.

Auf dieser Basis können wir gezielt auf die größten Risiken eingehen. Zum Beispiel mit den cloudnativen Sicherheitslösungen von Microsoft. Denn mit der Microsoft-Plattform managen Sie die verschiedenen Sicherheitsrisiken und sorgen dafür, dass Endanwender stets produktiv und sicher arbeiten.

Darüber hinaus bleiben Sie mit einer regelmäßigen Bewertung immer über die Cyber-Risiken innerhalb der Organisation informiert und wissen genau, welche möglichen Schwachstellen Sie dringend angehen müssen. Der beste Weg, um einen Aktionsplan auf der Grundlage von Fakten zu definieren.

Sie wollen wissen, wie es um Ihre Sicherheit steht? Dank unseres Cyber Security Assessment Tools (CSAT) sind Sie sich in kürzester Zeit aller digitalen Schwachstellen und Cyber-Risiken für Ihr Unternehmen bewusst.

Bitte wenden Sie sich für weitere Informationen oder einen Termin an QS solutions:

T: +49 (0)2234 – 69 00 0
E: info@qssolutions.de

solutions

Vereinbaren Sie hier Ihren persönlichen Beratungstermin:

https://qssolutions.de/produkte/cyber-security-assessment-tool/#demo