WIR STELLEN UNS VOR

AYSOME

IT Security GmbH

AYSOME
IT Security GmbH

VORWORT

- DAS ZEITALTER DER IT SECURITY -

Die Nutzung moderner IT zur Bewältigung von betriebswirtschaftlichen, logistischen und technischen Geschäftsprozessen sowie der Anschluss an das Internet sind heutzutage unabdingbare Erfordernisse, um im weltweiten Wettbewerb bestehen zu können. Digitalisierung und Vernetzung bergen jedoch neue Gefahren, die Unternehmen in ihrem Risikomanagement berücksichtigen müssen. Entsprechend sind Unternehmen - bei stetiger Zunahme von Missbrauch und Bedrohungen - auf Datenschutz und IT- Sicherheit angewiesen.
Eine gut organisierte IT Sicherheit vermindert die Anzahl der Schwachstellen, verringert die verbleibenden Risiken und begrenzt dadurch potentielle Schäden für das Unternehmen.
Leider sind die aktuellen Entwicklungen von erheblichen Ungleichgewichten geprägt. Die IT in den Unternehmen wird ständig ausgebaut und verbessert. Der IT Sicherheit hingegen wird leider häufig nicht der Stellenwert zugemessen, der ihr eigentlich gebührt und sie bleibt daher oft deutlich hinter den technologischen Entwicklungen zurück. Da sich auch die Cyberkriminalität jeden Tag weiterentwickelt, sollte Ihnen dieses Ungleichgewicht zu denken geben. Während die deutsche Regierung allmählich einen Ausbau der IT Sicherheit und eine stärkere Digitalisierung in Unternehmen fordert, bleibt es nur eine Frage der Zeit bis international standardisierte Normen der IT Sicherheit durch den Gesetzgeber für alle Unternehmen zur Verpflichtung gemacht werden. Besonders für wachsende und international ausgerichtete Unternehmen ist es empfehlenswert bereits heute Maßnahmen zu ergreifen und Ihr Unternehmen darauf vorzubereiten. Ein Ansporn für rechtzeitiges Handeln sollte auch aus finanzieller Sicht erfolgen – da die IT Sicherheit noch in den Startlöchern steht, können Unternehmen noch relativ kostengünstig von den IT Sicherheitsdiensten profitieren. Mit der verpflichtenden Gesetzgebung und dem damit wachsenden Bedarf an IT Sicherheit kann dies jedoch schon bald zu einem finanziell nicht haltbaren Problem für viele Unternehmen werden, an dem die Marktselektion und der Marktaustritt der Unternehmen ausgerichtet sein werden.

AYSOME
IT Security GmbH

Die AYSOME IT Security GmbH hat sich zum Ziel gemacht, unternehmensinterne Daten vor Cyber-Attacken zu schützen und mögliche Sicherheitslücken Ihres Unternehmens zu schließen. Zunehmende Angriffe auf IT-Systeme und Infrastrukturen haben die Digitalisierung von Unternehmen zum kritischen Erfolgsfaktor gemacht. Große Unternehmen und **insbesondere kleine sowie mittlere Unternehmen (KMU)** stehen im Bereich der IT Sicherheit vor erheblichen Herausforderungen. KMUs sind grundsätzlich keinen geringeren Risiken als große Unternehmen ausgesetzt, verfügen jedoch nur selten über vergleichbare Schutzmaßnahmen hinsichtlich der IT Sicherheit. Hierbei hat die Vergangenheit gezeigt, dass die infrastrukturellen IT Systeme mittelständischer Unternehmen in großem Maße hohe Sicherheitslücken aufweisen. Infolgedessen legen wir besonders den kleinen und mittelständischen Unternehmen ans Herz IT-Security Maßnahmen frühzeitig zu ergreifen. Unachtsamkeit und Unwissen im Umgang mit Systemen und ihren Anwendungen haben zur Folge, dass unzählige unternehmensinterne Daten an Außenstehende und Wettbewerber gelangen und Schäden in hohem Maße für Ihr Unternehmen bedeuten können.

- WIR WOLLEN IHNEN HELFEN SICH ZU SCHÜTZEN -

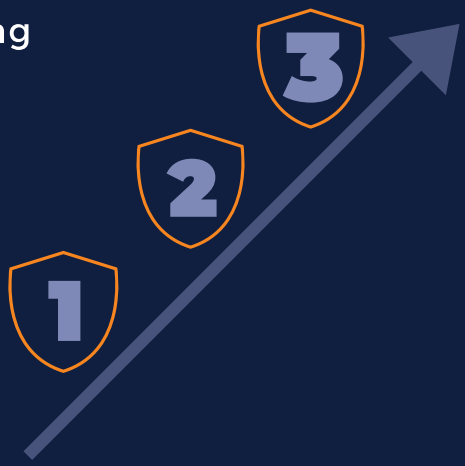
WER SIND WIR

Wir sind ein in Deutschland ansässiges Unternehmen mit dem Sitz in Düsseldorf. Unser Team arbeitet mit international ausgerichteten und sehr gut ausgebildeten IT-Spezialisten sowie IT-Projektmanagern aus der gesamten Europäischen Union zusammen. Kennzeichnend für unser Team ist der schnelle und flexible Einsatz unserer Spezialisten mit den stets höchsten Anforderungen an uns selbst. Wir konsultieren bereits erfolgreich unsere Partner und teilen unser Wissen mit großen Unternehmen aus der Europäischen Union und den Vereinigten Staaten.

AYSOME
IT Security GmbH

UNSERE LEISTUNG

Die AYSOME IT Security bietet Ihrem Unternehmen eine in drei Stufen untergliederte IT Security Dienstleistung. Die stufenartige Untergliederung bestimmt den Tiefgang der durchgeführten Maßnahmen zur Prüfung der IT Lücken und Sicherstellung des IT Schutzes Ihres Unternehmens. Jede der Stufen bietet einen optimal ausgewogenen Rahmen von Kosten und Nutzen der gewünschten IT Security.



1 HACK CHECK

Der Hack Check ist der Einstieg in die Welt der IT Sicherheit, der Ihnen die Notwendigkeit der IT Sicherheit und das Ausmaß infrastruktureller IT Schwachstellen Ihres Unternehmens aufzeigen kann. Dabei bietet die AYSOME IT Security Ihnen einen maschinellen **Vulnerability Scan** der IT Infrastruktur Ihres Unternehmens sowie eine anschließende Analyse und Beurteilung der Ergebnisse an.

Ein Vulnerability Scan ermöglicht hierbei das Scannen eines beispielsweise Computers oder Netzwerks und die Ermittlung von Schwachstellen und Sicherheitslücken in jenen Systemen. Hierfür wird eine Standard Vulnerability Management Software Nexpose und/oder Nessus eingesetzt. Der Scan verläuft über die gesicherte VPN/SSH Verbindung oder falls ausdrücklich erwünscht durch eine Installation eines lokalen Servers. Nachdem der Scan durchgeführt wurde, wertet unser Team die Daten aus. Anschließend erfolgen der Report und die Beurteilung des Hack-Checks.

Kostenpunkt: 999,00 Euro

AYSOME
IT Security GmbH

2 WEITERFÜHRENDE IT SECURITY

Mithilfe von weiterführenden IT Security Maßnahmen können wir beispielsweise zielgerichtete Analysen durchführen und ganz präzise Lösungen für die festgestellten Schwachstellen definieren.

Folgendes Spektrum an IT Security Maßnahmen bieten wir Ihnen an:

Installation und Konfiguration von Lösungen in den Bereichen

- o SIEM (Security Information and Event Management)
- o WAF (Web Application Firewall)
- o PAM (Priviledged Access Management)
- o VM (Vulnerability Management)
- o AV (Antivirus)
- o Firewall
- o Penetration Testing

uvm.

Dieses Angebot gilt für Unternehmen, die sich in einem Teilbereich der IT Security verbessern wollen.

Reporting & Lösungen

Projektmanagement und Human Resources Lösungen

Erläuterungen zu den einzelnen Maßnahmen folgen auf den nächsten Seiten.

Kostenpunkt: Auf Anfrage

AYSOME
IT Security GmbH

3 SPEZIALISIERTE IT SECURITY

Für Unternehmen, die einen Rundumschutz wünschen oder eine Zertifizierung im Bereich IT-Security anstreben, bieten wir die Möglichkeit sich nach **ISO/IEC 27001** zertifizieren zu lassen. In diesem Fall bietet die AYSOME IT Security den Aufbau, die Inbetriebnahme und/oder Audit einer Sicherheitslösung nach ISO/IEC 27001 an. Zu diesem Zweck werden unsere erfahrenen Spezialisten in allen Teilbereichen der Zertifizierung eingesetzt. Das bedeutet, wir bereiten für Sie die Zertifizierung für die Prüfstelle vor. Die Abnahme der Zertifizierung erfolgt durch einen Drittanbieter.

Wozu eine Zertifizierung nach ISO/IEC 27001?

Die meisten Firmen haben interne Sicherheitsrichtlinien für ihre IT. Durch eine interne Begutachtung (auch Audit genannt) können Unternehmen ihr korrektes Vorgehen im Abgleich mit ihren eigenen Vorgaben überprüfen. Die Unternehmen können damit allerdings ihre Kompetenzen im Bereich der IT-Sicherheit nicht öffentlichkeitswirksam gegenüber (möglichen) Kunden aufzeigen. Dazu ist eine Zertifizierung z. B. nach ISO/IEC 27001 auf Basis des IT-Grundschutzes sinnvoll. Eine Organisation hat die Möglichkeit, die Konformität zu einer Norm zu zeigen, indem ein unabhängiger externer Auditor die Konformität verifiziert: Dies wären wir in Ihrem Fall.

Was ist ISO/IEC 27001?

Die internationale Norm ISO/IEC 27001 spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits- und Managementsystems unter Berücksichtigung des Kontexts einer Organisation. Darüber hinaus beinhaltet die Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation und Anforderungen für die Implementierung von geeigneten Sicherheitsmechanismen, welche an die Gegebenheiten der einzelnen Organisationen adaptiert werden sollen. Die ISO/IEC 27001 wurde entworfen, um die Auswahl geeigneter Sicherheitsmechanismen zum Schutz sämtlicher Werte (Assets) in den Wertschöpfungsketten sicherzustellen. Mit der Digitalisierung, die in Deutschland fortschreitend gefördert wird und dem immer stärker belichteten Problem nach Datensicherheit ist es nur eine Frage der Zeit bis die Zertifizierung der Unternehmen nach Normen wie der ISO/IEC 27001 für die Unternehmen eine Verpflichtung wird.

Kostenpunkt: Auf Anfrage

AYSOME
IT Security GmbH

Erläuterungen der IT Security Maßnahmen

VM (Vulnerability Management)

+Mit dem Vulnerability Management (VM) sollen Prozesse und Techniken erarbeitet werden, mit denen zur Steigerung der IT-Sicherheit eine Sicherheitskonfiguration in Unternehmen eingeführt und verwaltet werden kann. Durch diverse Prozesse soll VM langfristig sichergestellt werden. Dazu gehört die regelmäßige Überprüfung des Netzwerks, des Firewall-Logging, durch Penetrationstests oder Virenscanner. Es erfolgt die Identifizierung der Schwachstellen durch Netzwerkanalysatoren und das Erkennen von Anomalien, die auf Angriffe mit Malware oder auf andere böswillige Attacken hindeuten sowie ihrer Auswirkungen auf Server, Anwendungen, Netzwerke oder Systeme. Außerdem muss das Risiko klassifiziert werden. In einem weiteren Prozess wird untersucht, wie Schwachstellen verhindert und beseitigt werden können. Da sich die Bedrohungen ständig weiterentwickeln, müssen die Strategien des VM regelmäßig aktualisiert werden, um den ändernden Bedrohungsszenarien gerecht zu werden.+

SIEM (Security Information and Event Management)

SIEM = SEM+SIM

+ Das SEM-System ermöglicht ein gebündeltes Speichern und Interpretieren von gesammelten Daten. Somit kann die Datenanalyse praktisch in Echtzeit durchgeführt werden. Infolgedessen sind die notwendigen Schutzmaßnahmen schnell einleitbar. Bei dem SIM-System erfolgt eine zentrale Datensammlung für Analysezwecke, welche folglich die Erstellung von automatisierten Berichten bezüglich der IT-Compliance sowie ein zentralisiertes Berichtwesen gestattet. Das Zusammenbringen von SEM und SIM erschafft mit SIEM ein System, das eine rasche Lokalisierung, Analyse und Beseitigung von sicherheitsbedrohlichen Ereignissen ermöglicht. +

WAF (Web Application Firewall)

+ Über die WAF erhalten Ihre Webanwendungen Schutz vor Angriffen über das Hypertext Transfer Protocol (HTTP). Die WAF inspiziert dabei alle eingehenden und ausgehenden Aktionen des Web-Servers. Sobald die Aktionen verdächtig scheinen, wird der Zugriff unterbunden. Eine Vielzahl verschiedener Bedrohungen kann damit abgewehrt werden. Darunter finden sich SQL Injection Angriffe, Script Injection Angriffe, Angriffe per Cross-Site Scripting (XSS), Angriffe per Pufferüberlauf oder Parameter und Hidden Field Tampering. Cookie Poisoning oder der unbefugte Zugriff auf bestimmte Bereiche des Webservers und Identitätsdiebstahl können ebenso vermieden werden. +

AV (Antivirus)

+Durch die Antivirus Maßnahmen werden Computerviren, Computerwürmer und Trojanische Pferde aufgespürt, blockiert und beseitigt.+

PAM (Priviledged Access Management)

+Das PAM schützt Ihr Unternehmen vor vorsätzlichem, aber auch unbewusstem Missbrauch privilegierter Zugänge. Besonders wachsende Organisationen profitieren von derartigen Lösungen, da IT-Netzwerke und Systeme mit zunehmendem Wachstum immer komplexer werden. Die Anzahl der Mitarbeiter, Dienstleister und Nutzer wächst unkontrolliert. Manche dieser Administratoren überschreiben existierende Sicherheitsprotokolle. Dadurch entstehen große Schwachstellen. Wenn solche privilegierten User ohne jegliche Kontrolle das System verändern oder Daten kopieren können, stellt dies eine potenzielle Bedrohung für jede Organisation dar. Einerseits besteht die Gefahr von „Inside-Jobs“, also das Risiko, dass ein Angestellter oder ein Dienstleister bewusst Informationen stiehlt oder das Netzwerk sabotiert. Andererseits können auch Cyberkriminelle Zugangsdaten entwenden und als Mitarbeiter getarnt in Netzwerke eindringen. PAM löst dieses Problem.+

Firewall

+Die Firewall ist ein Sicherungssystem, welches ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Weiter gefasst ist eine Firewall auch ein Teilaspekt eines Sicherheitskonzepts. Jedes Firewall-Sicherungssystem basiert auf einer Softwarekomponente. Die Firewall-Software dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender oder Ziel und genutzten Diensten. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden dürfen oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden.+

Penetration Testing

+Der Penetrationstest ist der fachsprachliche Ausdruck für einen umfassenden Sicherheitstest einzelner Rechner oder Netzwerke jeglicher Größe. Unter einem Penetrationstest wird die Prüfung der Sicherheit möglichst aller Systembestandteile und Anwendungen eines Netzwerks oder Softwaresystems mit Mitteln und Methoden verstanden, die ein Angreifer (ugs. „Hacker“) anwenden würde, um unautorisiert in das System einzudringen (Penetration). Der Penetrationstest ermittelt somit die Empfindlichkeit des zu testenden Systems gegen derartige Angriffe. Wesentlicher Teil eines Penetrationstests sind Werkzeuge, die dabei helfen, möglichst alle Angriffsmuster nachzubilden, die sich aus den zahlreichen bekannten Angriffsmethoden herausbilden. Die Art der Sicherheitstests orientiert sich am Gefahrenpotential eines gefährdeten Systems, Netzwerks oder einer Anwendung. Die Differenzierung der Tests ergibt sich aus dem Kontext, dass beispielsweise ein Webserver eine höhere Gefahrenpriorität als eine einfache Textverarbeitung hat.+

AYSOME
IT Security GmbH

REPORTING

Das Reporting wird als Instrument im Qualitätsnachweis vom IT Service eingesetzt. Dabei achten wir sorgsam auf eine inhaltlich genaue Darstellung und sinngemäße Strukturierung aller Kennzahlen für ein besseres Verständnis. Hierbei werden Schlüsselindikatoren, die in prozessbezogene (Gesamt-Performance), operative (Performance-Bewertung der Komponenten z.B. CPU Auslastung) und service-/businessbezogene (Performance von Diensten z.B. SAP-Service; kundenrelevante Daten) unterteilt werden, aufgeführt. Weiterhin werden unsere Reports nach Zielgruppen differenziert, um das Reporting dem Informationsinteresse nach darzulegen. Ob IT Leiter oder Prozess Manager – Sie erhalten von uns ein zugeschnittenes Reporting mit den für Sie besonders relevanten Kennzahlen für eine schnelle und effiziente Informationsausstattung.

PROJEKTMANAGEMENT UND HUMAN RESOURCES LÖSUNGEN

Mit unserem IT-Projektmanagement bieten wir die Planung, Organisation und Steuerung informationstechnische Projekte. Wir koordinieren alle beteiligten Mitarbeiter, Abteilungen und externe Dienstleister. Während der Umsetzung behalten wir den Zeitplan und das Budget immer im Blick. Indem wir die doppelte Verantwortung übernehmen und somit nicht nur die Ausführung, sondern auch die Zielerreichung in der Hand haben, bürgen wir für ein einwandfreies Ergebnis des von Ihnen gewünschten Projekts. Unsere Devise: Mit so vielen Ressourcen wie nötig und so wenigen wie möglich das beste Ergebnis herauszuholen.

Ob zwischen System Operatoren, dem leitenden Architekten, Chefdesigner oder Qualitätsmanager – unser IT-Projektmanagement bildet die perfekte Schnittstelle und fördert die Zusammenarbeit und den Austausch zwischen den Fachabteilungen. Wir definieren mit Ihnen zusammen Ziele, erstellen Release-Pläne und kümmern uns um die Aufgabenverteilung. Zudem sorgen wir dem Projekt und Unternehmen entsprechend sinnvolle Werkzeuge, Plattformen, Entwicklungsumgebungen, Architekturen und Programmiersprachen.
Wir sind Ihr unternehmensinterner Ansprechpartner. Durch die Kombination informationstechnischen und betriebswirtschaftlichen Wissens, sind wir bestens vorbereitet Ihrem Projekt Leben einzuhauchen.

KONTAKT & IMPRESSUM

AYSOME IT Security GmbH
Benzenbergstraße 2
40219 Düsseldorf
Deutschland
E-mail: info@aysome.com

www.aysome.com

vertreten durch die Geschäftsführung: Georg Kolesnikovic
unter der oben genannten Anschrift der AYSOME IT Security GmbH.

Registergericht: Amtsgericht Düsseldorf
Registernummer: HRB 83383

Verantwortlicher nach § 55 RStV:

Georg Kolesnikovic
Benzenbergstraße 2
40219 Düsseldorf
E-mail: info@aysome.com