it südwestfalen
Wir machen Ihre IT verfügbar!

IT-Sicherheit

- Informationssicherheit
- Notfallmanagement
- Firewalling
- Virenschutz
- Datensicherung & Backup
- Datenschutz

Schützen Sie das Wichtigste in Ihrem Unternehmen: Ihre Daten!

Informationssicherheit

Sicherheit und Verfügbarkeit Ihrer Daten

Informationssicherheit über die gesamte Wertschöpfungskette hinweg

Warum Informationssicherheit?

Unter Informationssicherheit wird häufig ein funktionierender Virenschutz, eine Firewall sowie eine vorhandene Datensicherung verstanden. Sicherlich handelt es sich dabei um wichtige Bestandteile eines ganzheitlichen Informationssicherheitskonzeptes, betrachtet dieses jedoch nur punktuell. Zum einen gilt es zunächst die erwähnten Komponenten zu beurteilen und zu analysieren. Dabei müssen verschiedenste Fragen beantwortet werden. Wird die Datensicherung nach der 3-2-1-Regel durchgeführt (siehe Seite 32)? Welche Aufbewahrungsfristen habe ich für meine Backups? Sind meine mobilen Endgeräte geschützt? Und viele mehr.

Das Thema Informationssicherheit ist jedoch wesentlich komplexer und nicht nur auf diese wenigen Komponenten zurückzuführen. Es stellen sich viele weitere Fragen. Wie sicher sind Ihre Gebäude, Systeme, Anwendungen, Daten und auch Ihr Personal? Wie Sie sehen beurteilt die Informationssicherheitsanalyse auch organisatorische Prozesse. Nach einer umfangreichen Analyse Ihrer Strukturen erstellen wir ein organisatorisches Konzept und ermitteln den Schutzbedarf. Wir führen in Ihrem Unternehmen einen Basis Sicherheits-Check durch und erstellen einen Maßnahmenkatalog, der sich an die VdS & ISO-Standards anlehnt. Dieser zeigt Ihnen auf Basis von definierten Handlungsfeldern den Handlungsbedarf mit konkreten Maßnahmen.

Einflussfaktoren auf die IT-Sicherheit

- Höhere Gewalt
- Vorsätzliche Handlungen
- Technisches Versagen
- Wettbewerb
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Gesetze und Compliance von Kunden und Lieferanten

Notfall-Management

Zwar werden häufig vielerlei Maßnahmen für die Informationssicherheit getroffen, ein dokumentiertes Notfallmanagement hingegen existiert in den meisten Fällen nicht. Dabei ist es wichtig, dass im Notfall nach einem konkreten Plan und nicht willkürlich gehandelt wird. Dies erspart Schäden und Ausfallzeiten.

Wir identifizieren und dokumentieren deshalb Ihre kritischen Prozesse. Für diese wird dann nach Risikoart eine Notfallplanung mit entsprechenden Wiederanlaufplänen erarbeitet. Parallel dazu wird ein Notfallhandbuch erstellt, nach welchem die IT-Verantwortlichen, Geschäftsleitung und Mitarbeiter handeln können.

Bin ich zur Informationssicherheit verpflichtet?

Der Bundestag beschloss am 12.06.2015 das IT-Sicherheitgesetz. Dadurch sollen die Betreiber besonders gefährdeter Infrastrukturen verpflichtet werden IT-Sicherheit im Unternehmen zu etablieren. Der Schutz von Vermögenswerten betrifft aber auch durch andere gesetzliche Vorgaben jeden Unternehmer, unabhängig von Firmengröße oder Bedeutung für die Bundesregierung. In der Haftung für jegliche Schäden steht immer die Geschäftsführung.

Penetrationstests

Wir führen regelmäßig Penetrationstests sowohl einzelner Geräte, wie Ihrer Firewall, als auch des gesamten Serverraums durch. Wir simulieren echte Ausfallszenarien und finden somit kontrolliert heraus, ob Sie für verschiedene Disaster-Fälle gerüstet sind.

Mitarbeiter Sensibilisierung

Das eigene Personal stellt gerade im Zeitalter von Wirtschaftsspionage und Verschlüsselungstrojanern eine echte Gefahr für die Informationssicherheit dar. Deshalb ist es wichtig Ihre Mitarbeiter zu sensibilisieren. Durch Workshops wird nicht nur das Gefahrenpotential aufgezeigt, sondern auch die Möglichkeiten zur Erkennung und Vermeidung. Um der Sensibilisierung die nötige Nachhaltigkeit zu geben, versenden wir auf Wunsch im Nachgang E-Mails, die täuschend echt sind, jedoch keine Schadsoftware enthalten. Stattdessen zählt ein Counter, wir häufig die E-Mail innerhalb Ihres Unternehmens geöffnet wurde.

Übernehmen Sie Verantwortung für die Sicherheit des wichtigsten Gutes Ihres Unternehmens- Ihre Daten!

„Schützen Sie das wichtigste Ihres Unternehmen! Ihre Daten!“

Quick Check & Quick Audit als optimale Grundlage

Quick Check

Durch den Quick-Check nach VdS, beschreiben Sie zunächst durch Selbstauskunft den aktuellen IST-Zustand Ihres Unternehmens in Bezug auf den Cyber-Security-Status. Die Basis bildet hierbei die VdS Richtlinie 3473.

Um sinnvolle Maßnahmen für Ihr Unternehmen zu gewährleisten, sind wahrheitsgemäße Angaben im Quick-Check Voraussetzung. Hierbei beantworten Sie in unserem Beisein insgesamt 39 Fragen aus den Bereichen Organisation, Technik, Prävention und Management. Folgend wird die danach von uns erstellte Matrix zur Auswertung samt standardisierter Maßnahmenempfehlungen per E-Mail an Sie versendet.

Quick Audit

Das Quick-Audit wird auf derselben Basis an Fragen wie der Quick-Check durchgeführt. Durch eine intensivierte und genauere Angabe ist die Auswertung jedoch präziser und die folgende Maßnahmenempfehlung individuell auf Ihre Situation bezogen.

Hat bestimmtes Personal beispielsweise Zugang zu sensiblen Informationen, kann sich als Maßnahme ein Zugriffsschutz für diese Informationen eignen. Ist es in einem Unternehmen erlaubt private Geräte mit dem Netzwerk zu verbinden, kann je nach Situation ein Verbot, bis hin zur Einrichtung eines speziell dafür erstellten Netzwerks die richtige Lösung sein. Die Ergebnisse werden zudem samt Empfehlungen von uns präsentiert.

Jörg Zimmer, Ihr Ansprechpartner

Herr Jörg Zimmer ist Leiter und Berater für Informationssicherheit bei der IT Südwestfalen AG. Sein Fokus liegt dabei auf der ganzheitlichen Analyse der IT des Kunden. Neben einem umfassenden IT-Sicherheitscheck mit anschließendem Sicherheitskonzept, erarbeitet Herr Zimmer ebenfalls ein Notfall-Management. Neben der IT-Sicherheit hat Herr Zimmer umfassende Erfahrungen im Bereich IT-Infrastruktur, IT-Strategie sowie in der IT-Organisation und dem Prozessmanagement. Zuvor hat er mehr als 22 Jahre bei einer renommierten Bank als Leiter der IT gearbeitet.

Schwerpunkte

- 25 Jahre IT-Erfahrung, 17 Jahre in leitender Position
- 12 Jahre Erfahrung im Bereich Informationssicherheit und Notfallmanagement
- Ehemaliger Dozent der Sparkassenakademie Münster
- Organisation & Projektmanagement
- IT-Strategie und IT-Infrastrukturplanung

Zertifizierungen

- VdS anerkannter Berater für Cyber-Security
- Auditor nach ISO 27001 (TSG)
- ITIL Foundation
- Kaspersky, VMWare, Veeam Zertifikate

Sicherheit ist kein unveränderbarer Zustand, der einmal erreicht wird und sich niemals wieder ändert.

Datensicherung

Maximale Verfügbarkeit Ihrer Daten

Maximieren Sie die Verfügbarkeit Ihrer Daten

3-2-1 Regel der Datensicherung

Eine allzeit gültige Regel, mit der Sie in beliebigen Ausfallszenarien vor Datenverlust geschützt sind, ist die 3-2-1-Regel der Datensicherung. Sie liefert zugleich auch die Antwort auf zwei wichtige Fragen: Wie viele Backup-Dateien sollten erstellt und wo sollten diese aufbewahrt werden? Grundsätzlich gibt es zwei Gruppen von Menschen: Menschen, die bereits von einem Speicherausfall betroffen waren und Menschen, denen ein solcher Ausfall noch bevorsteht. Die 3-2-1-Regel der Datensicherung besagt:

3 Kopien Ihrer Daten

Drei Kopien bedeuten, dass zusätzlich zu den primären Daten mindestens zwei weitere Backups vorhanden sein sollten. Doch warum reicht ein Backup nicht aus? Wenn Sie mehrere Kopien Ihrer Daten aufbewahren, ist folglich auch das Risiko eines Datenverlusts bei einem schwerwiegenden Ausfall um ein vielfaches geringer.

2 unterschiedliche Medien

Die Geräte, auf denen Sie Ihre Datenkopien speichern, fallen niemals aus denselben Gründen aus. Diese Voraussetzung lässt sich naturgemäß nicht erfüllen, wenn Sie für Ihre primären Daten und das Backup denselben Speicherort wählen. Zudem kommt es nach einem Ausfall einer Festplatte häufiger vor, dass kurz darauf eine weitere Festplatte desselben Speichersystems ausfällt. Aus diesem Grund besagt die 3-2-1-Regel, dass Sie Kopien Ihrer Daten auf mindestens zwei unterschiedlichen Speichertypen aufbewahren sollten, beispielsweise auf einem internen Festplattenlaufwerk UND einem NAS-System.

1 externer Speicherort

Von entscheidender Bedeutung ist es die Kopien physisch voneinander getrennt aufzubewahren. Es ist nicht empfehlenswert, das externe Speichergerät in dem Raum aufzubewahren, in dem sich auch das Produktivspeichersystem befindet. Bei einem Brand wären alle Daten unwiederbringlich verloren. In Unternehmen wird entweder eine Sicherung auf externen Festplatten vorgenommen, die an einem externen Ort aufbewahrt werden oder es wird ein Backup in die Private Cloud gemacht.

Veeam vs. klassische Backup-Software

Klassische Datensicherungssoftware haben mehrere Nachteile: „Das eine Datensicherung korrekt durchgelaufen ist, bedeutet im Umkehrschluss nicht, dass diese auch zurückgesichert werden kann.“ Im Klartext bedeutet dies, dass Sie ohne regelmäßige aufwändige Tests der klassischen Datensicherung keine Garantie auf rücksicherbare Daten haben. Klassische Backupsoftware ist zudem sehr wartungsintensiv. Nach jeglicher Änderung muss auch der Datensicherungsjob angepasst werden. Dieses Prinzip ist fehleranfällig. Auch die Zeiten für eine Rücksicherung sind enorm, so dass hier mit langen Ausfallzeiten gerechnet werden muss. Die empfohlene Datensicherungssoftware Veeam sichert immer die gesamte virtuelle Maschine, mit all seinen Einstellungen und Anwendungen. Dabei spielt es keine Rolle mehr, was sich auf dem Server ändert. Veeam arbeitet neben klassischen Backups außerdem mit sogenannten Replikationen, startbaren Sicherungen. Im Falle eines Ausfalls der produktiven Hardware, können auf Knopfdruck die virtuellen Maschinen auf dem Backup Server gestartet werden.

Veeam Private Cloud Backup

Als offizieller Veeam Cloud & Service Provider können Sie die Ressourcen der IT Südwestfalen AG im Lüdenscheider Rechenzentrum als Backup-Ziel nutzen und so Ihre Backups oder auch Replikationen (startbare Sicherungen) verschlüsselt über die Internetleitung transferieren. Auf Wunsch kann dies auch auf ein eigenes NAS oder einem eigenen Backup-Server erfolgen. Und das bereits ab 49 € monatlich. Mehr dazu auf Seite 21.

Highlights

- Schnellste Wiederherstellung von ganzen virtuellen Maschinen, einzelner Dateien oder Anwendungsobjekte
- Mit Replikationen stehen auf Knopfdruck startbare Sicherungen und Server zur Verfügung
- Dank SureBackup sind Ihre Sicherungen in jedem Fall rücksicherbar. Dies prüft die Software automatisch.
- Durch die integrierte WAN-Beschleunigung lassen sich Backups bis zu 50 Mal schneller an andere Standorte übertragen.
- Zuverlässige Sicherung auch von Endpoints

Datenverfügbarkeit so zuverlässig wie nie!

"Daten sind Ihr wichtigstes Gut, weshalb die Verfügbarkeit dieser auch im Falle eines Ausfalls an oberster Stelle steht."

VEEAM | CSPPARTNER Silver

VEEAM | PROPARTNER Silver Reseller

Veeam Backup & Replication

	Standard	Enterprise	Enterprise Plus
VMware vSphere und Microsoft Hyper-V kompatibel	✓	✓	✓
Backup inkl. integrierter Deduplizierung & Komprimierung	✓	✓	✓
Wiederherstellung (virtuelle Maschinen, virtuelle Festplatten, Dateiebene)	✓	✓	✓
Replikationen (Startbare Sicherungen)	✓	✓	✓
End-to-end-Verschlüsselung (während des Backups, während der Übertragung & bei der Speicherung)	✓	✓	✓
Veeam Cloud Connect für Backups und Replikationen (schnelles & sicheres Cloud-Backup)	✓	✓	✓
SureBackup® und SureReplica (Prüfung auf Rücksicherbarkeit)	✗	✓	✓
On-Demand Sandbox™	✗	✓	✓
Erweiterte Wiederherstellung für Microsoft Active Directory, Exchange, SharePoint & SQL-Server	✗	✓	✓
Erweiterte Verschlüsselung (Schutz bei Passwortverlust)	✗	✓	✓
WAN-Beschleunigung (für Veeam Cloud Connect)	✗	✓	✓
WAN-Beschleunigung (für andere externe Backup-Ziele)	✗	✗	✓
Self Service Portal	✗	✗	✓
Aufgabenautomatisierung	✗	✗	✓
Lizenzkosten exemplarisch für einen CPU-Sockel inkl. 1 Jahr Support und Service seitens Veeam	650 € Einmalig	1.150 € Einmalig	1.900 € Einmalig

Ihr Weg zur optimalen Datensicherung

1 Erstgespräch & Workshop

Das Vorgehen

- Erstgespräch
- Aufnahme des IST-Zustandes
- Vorstellung technischer Möglichkeiten
- Erarbeitung & Dokumentation Ihrer Anforderungen & Ergebnisse
- Beratung, Auswahl und Empfehlung des richtigen Produktes

2 Konzept & Installation

Das Vorgehen

- Erarbeitung Ihres individuellen Datensicherungs-Konzeptes auf Basis des Workshops
- Vorbereitung & Installation der Software
- Umsetzung des dokumentierten Konzeptes
- Durchführung von Tests
- Dokumentation der Lösung

3 Schulung & Inbebetriebnahme

Das Vorgehen

- Einweisung und Schulung Ihrer Mitarbeiter
- Inbetriebnahme der Lösung & Durchführung der Initialsicherung
- Regelmäßiger Austausch nach Einführung der Lösung
- Auf Wunsch Monitoring Ihrer Datensicherung durch uns

Mit Veeam Cloud Backup sichern Sie Ihre Daten ins hochsichere Rechenzentrum im Gebäude der Stadtwerke Lüdenscheid!

Angebote nur für Gewerbetreibende. Preise zzgl. gesetzlicher MwSt.

Virenschutz

Maximale Sicherheit für Ihre Daten

KASPERSKY lab Gold Partner

TREND MICRO Bronze Partner

Schützen Sie sich vor Viren, Malware und Trojanern

Das richtige Konzept ist entscheidend

Im Zeitalter der Verschlüsselungstrojaner hat die Quantität und vor allem die Qualität der Bedrohungen enorm zugenommen. Im Falle eines Befalls werden sämtliche Dateien auf PCs und Servern verschlüsselt. Ziel der Erpresser ist es meist Geld zu erbeuten, weshalb gegen eine Lösegeldzahlung ein Entschlüsselungsprogramm versprochen wird, welches jedoch in wenige Fällen Abhilfe schafft. Es drohen also Betriebsausfälle sowie Datenverlust. Die finanziellen und Image-Schäden können ein enormes Ausmaß annehmen.

Um Schäden zu vermeiden oder wenigstens so gering wie möglich zu halten, ist ein ausgefeiltes auf Sie zugeschnittenes IT-Sicherheitskonzept unabdingbar. Dieses beinhaltet neben einem Datensicherungs- und Firewalling-Konzept einen Virenschutz. Es werden Ihre Anwendungsszenarien sowie Hard- und Software analysiert. Auf Basis dieses Konzeptes ermitteln wir gemeinsam mit Ihnen das passende Produkt, welches auf Ihre Anwendungsfälle zugeschnitten ist.

Auf Wunsch führen wir mit Ihnen gemeinsam ein Proof of Concept durch und setzen das erarbeitete Konzept in einer Testumgebung um. Dadurch lassen sich Leistungsfähigkeit und Anforderungen auf Herz und Nieren prüfen. Durch gezielte Workshops machen wir Ihre IT-Verantwortlichen mit den Möglichkeiten und dem Handling der Software vertraut, damit Sie sicher geschützt sind.

Plattformunabhängiger Schutz

Es werden sämtliche PCs, Notebooks und Server gesichert. Windows, Mac und Linux werden vollumfänglich unterstützt.

Mobiler Schutz für Smartphone & Tablet

Verschwundene Geräte können gesperrt, gelöscht und ausfindig gemacht werden. Vertrauliche Geschäftsdaten werden in sicheren Containern gesichert. Mehr zum Thema Mobile Device Management erfahren Sie auf Seite 37.

Anti-Cryptor gegen Ransomware

Bei einer versuchten schädlichen Verschlüsselung wird automatisch eine Sicherung und Wiederherstellung der entsprechenden Datei ausgelöst. Das betroffene Gerät wird automatisch vom Netzwerk getrennt und bereits die Verschlüsselung der ersten Datei wird rückgängig gemacht.

Schnelle Performance

Je nach Anzahl der aktivierten Schutz-Komponenten ist die Performance ein großes Thema. Bei den Produkten von Kaspersky und Trend Micro ermöglicht die Software-Leistung einen effektiven Datenverkehrsstrom, schnellere Web-Ladezeiten und optimierte Deployments, Updates und Startzeiten.

Virenschutz & mehr für Ihr Smartphone?
Mobile Device Management
Seite 37

Vertrauen Sie Ihrem IT-Sicherheitsexperten der Region!

"Mit dem Managed Anti-Virus müssen Sie sich nie wieder Gedanken um die Aktualität und Verfügbarkeit Ihres Virenschutzes machen!"

Managed Anti-Virus: Virenschutz as a Service

Warum Managed Anti-Virus?

Einen installierten Virenschutz zu haben, bedeutet im Umkehrschluss nicht gleich optimal geschützt zu sein. Das trifft vor allem kleine Unternehmen, die keine eigene IT-Abteilung haben.

Unternehmen ohne einen eigenen IT-Verantwortlichen haben häufig das Problem, dass sie die Software auf dem Server nach der Installation durch den Dienstleister nicht administrieren und warten. Die Folge können eine veraltete Software und Signaturen sowie nicht erkannte Bedrohungen an den Servern oder Clients sein. Denn nur in den seltensten Fällen schauen Geschäftsführer in die Administratorkonsole der Anti-Virensoftware, um zu prüfen, ob auf dem Server Schadsoftware gefunden wurde oder ob alle Arbeitsplätze mit aktuellen Virensignaturen versorgt werden. Meist fallen solche Sicherheitslücken erst zu spät auf.

Das Managed Anti-Virus basiert auf der vielfach ausgezeichneten und leistungsfähigen Engine von Kaspersky.

Sie müssen nie wieder die Wartung für ein Produkt nachkaufen, da diese bereits im Service enthalten ist. Neben der reinen Software-Lizenz beinhaltet das Managed Anti-Virus auch das Monitoring des Virenschutzes. Server und Clients werden durchgängig auf Bedrohungen sowie Aktualität des Schutzes geprüft. Demnach sorgen wir mehrfach täglich für aktuelle Virenschutz-Signaturen auf allen Geräten. Sollte es auf einem Server oder Client zu einer Bedrohung oder gar einem Befall kommen, werden die Sicherheitsexperten unseres Hauses aktiv und setzen sich mit Ihnen in Verbindung, um das Problem schnellstmöglich einzugrenzen und zu beheben.

Durch den Betrieb sowie der Verwaltung des Management-Servers in einem hochsicheren regionalen Rechenzentrum durch uns, sparen Sie zudem IT-Ressourcen, die Sie für andere Szenarien nutzen können. Außerdem gilt: Jeder (virtuelle) Server, der nicht vorhanden ist, muss auch nicht gewartet werden. Sie sparen sich Lizenzen für das Betriebssystem sowie die Kosten für die Wartung des Servers.

Managed Anti-Virus	**Standard**
Effektiver Schutz vor Viren, Spyware & Malware	✓
Tägliche Überprüfung des Sicherheits-Status (Bedrohungen & Signaturen)	✓
Mehrfach täglich Updates der Schutz-Signaturen	✓
Updates der Agenten auf die aktuelle Version	✓
Betrieb und Verwaltung eines zentralen Management-Servers im hochsicheren Rechenzentrum	✓
Unterstützung von PCs & Notebooks (Windows, Linux, Mac)	✓
Unterstützung von Servern (Windows, Linux, Mailserver) inkl. Anti-Cryptor gegen Ransomware für Fileserver	✓
Regelmäßiges Audit nach ungeschützten Geräten	✓
Alarmierungsart im Bedrohungsfall (situationsabhängig)	E-Mail / Telefon
Einmalige Bereitstellungsgebühr (zzgl. individueller Einrichtung)	9,90 €
Kosten je Node Ab 25 Lizenzen: 5% Rabatt Ab 50 Lizenzen: 10% Rabatt	5 € Monatlich

Virenschutz as a Service: Einfach, sicher, unkompliziert

So einfach war Virenschutz noch nie!

Firewalling

Mehr als Netzwerksicherheit

Sophos Silver Partner

Cisco Select Partner

Sicherheit und Verfügbarkeit für Ihr Netzwerk

Warum eine Firewall Pflicht ist

In jedem Sicherheitskonzept sollte eine Firewall berücksichtigt werden, da ein vorhandener Router sowie ein Virenschutz alleine nicht genügen. Ein Virenschutz und eine Softwarefirewall auf dem Computer erkennen bei weitem nicht alle Bedrohungen und wenn ein Virenschutz Alarm schlägt, hat der Schädling bereits einen Weg durch das Internet in Ihr Netzwerk gefunden. Unter Umständen wurden zu diesem Zeitpunkt bereits andere Geräte befallen. Deshalb ist es wichtig das Unternehmensnetzwerk vor dem Internet zu schützen und nur die notwendigen Ports zu öffnen.

Weiter dient eine Firewall nicht nur zum Schutz vor dem Internet, sondern bietet weitere Services, die für einen sicheren Unternehmensbetrieb notwendig sind, angefangen vom sicheren WLAN bis hin zur Anbindung des Außendienstes.

Die richtige Konfiguration ist entscheidend

Bei der Konfiguration einer Firewall kann viel falsch gemacht werden. Wichtig ist es deshalb die Anforderungen des Unternehmens und der Nutzer zu analysieren sowie zu bewerten. Es werden sowohl Ihre Compliance als auch Datenschutzbestimmungen berücksichtigt. Dabei geht es beispielsweise um die interne Nutzung des Internets, die Anbindung des Außendienstes oder der Vernetzung mehrerer Standorte, bis hin zum Datenaustausch mit Kunden und Lieferanten. Erst im Anschluss wird das richtige Gerät für Sie ermittelt und ein Konfigurationsplan erstellt.

Managed Firewall

Die Wartung und das Management einer Firewall kann nur durch sachkundiges Personal erfolgen, welches sich regelmäßig mit dem Thema auseinandersetzt. Hinzu kommt eine kostenpflichtige und regelmäßige Erneuerung der Services, damit Sie sowohl aktuelle Sicherheitsfeatures als auch den Support seitens des Herstellers nutzen können.

Mit dem Produkt Managed Firewall stellen wir Ihnen für eine monatliche Pauschale eine virtuelle oder dedizierte Firewall-Appliance zur Verfügung. Wir übernehmen für Sie sowohl die Ersteinrichtung als auch die regelmäßige Wartung und das Management. Dabei passen wir sämtliche Konfigurationen nach Ihren Wünschen an.

Durch unser integriertes Monitoring überprüfen wir laufend die Funktionalität der Firewall mit den einzelnen Services. Somit können Sie sich stets sicher sein eine funktionierende VPN-Verbindung und die aktuellste E-Mail-Security zu nutzen. Wir konzentrieren uns auf Ihre Firewall, damit Sie sich auf Ihr Business konzentrieren können!

Wichtige Sicherheitsfeatures

- Überwachung von Anwendungen
- Sicherer Remotezugriff
- WLAN-Absicherung
- Sichere und optimale Anbindung des Außendienstes
- Sicherheit für Ihre Webanwendungen
- E-Mail-Sicherheit
- Schutz vor Gateway-Bedrohungen
- Einfache Administration

Vertrauen Sie Ihrem IT-Sicherheitsexperten der Region!

Mobile Device Management

Schützen Sie Ihre Unternehmensdaten

vmware airwatch

vmware PARTNER ENTERPRISE SOLUTION PROVIDER

vmware SERVER VIRTUALIZATION | CLOUD PROVIDER | ACADEMIC SPECIALIZATION | MOBILITY MANAGEMENT

KASPERSKY Gold Partner

IT-Sicherheit
- Informationssicherheit
- Datensicherung
- Virenschutz
- Firewalling
- Mobile Device Management
- Security Trainingsplattform
- Datenschutz

Schützen Sie Ihre Unternehmensdaten auf mobilen Endgeräten

Warum Mobile Device Management?

Unternehmen investieren regelmäßig in IT-Sicherheitsmaßnahmen. Beim Blick auf das WLAN-Netzwerk fallen eine Vielzahl von mobilen Endgeräten auf, darunter Smartphones und Tablets. Diese werden meist nicht ausreichend geschützt. Dabei werden diese häufig für den Außendienst genutzt und sowohl Adressdaten, E-Mails, Kalendereinträge, als auch sensible Dokumente werden gespeichert.

Die meisten dieser Geräte weisen enorme Sicherheitsmängel auf und sind für die geschäftliche Nutzung nicht geeignet. Die Vielzahl an Geräten verschiedener Hersteller mit unterschiedlichen Betriebssystemen (Android, iOS, Windows Phone) und Versionen erschweren die IT-Sicherheit und gefährden Ihre Daten enorm. Wenn dann eines dieser Geräte infiziert ist oder gar gestohlen wird, ist dieser Schaden kaum zu regulieren.

Zudem ist die manuelle Administration für IT-Abteilungen intransparent und zeitaufwendig und kostet dem Unternehmen viel Geld. Es gibt also viele gute Gründe sich abzusichern!

Datenschutz Grundverordnung DSGVO

Die am 25.05.2018 in Kraft getretene EU-Datenschutz-Grundverordnung schreibt vor, dass neben Notebooks auch mobile Endgeräte, wie Tablets und auch Smartphones vor Missbrauch geschützt werden müssen. Dabei genügt die reine Pineingabe nicht. Vielmehr muss der Speicher des jeweiligen Betriebssystems verschlüsselt und damit vor unbefugtem Zugriff geschützt werden. Das ist bei neuen Smartphonemodellen standardmäßig der Fall. Der Schutz von Unternehmensdaten sollte nicht nur im Zuge der DSGVO, sondern auch im Interesse eines jeden Unternehmens durchgeführt werden.

"Schützen Sie Ihre Unternehmensdaten vor Missbrauch"

Managed MDM — Basic

Mobiler Malwareschutz (Android) & Web-Filter (Android & iOS)	✓
Rooting- & Jailbreak-Schutz	✓
Standortermittlung & Fernlöschung bei Verlust möglich	✓
Verteilung von E-Mail & WLAN-Einstellungen möglich	✓
Apps erlauben & verbieten (Android)	✓
Self Service Portal (auf Anfrage)	✓
Updates der Agenten auf die aktuelle Version	✓
Betrieb und Verwaltung eines zentralen Management-Servers im hochsicheren Rechenzentrum	✓
Unterstützung von Android, iOS & Windows 10 Mobile	✓
Einmalige Bereitstellungsgebühr (zzgl. Individuelle Einrichtung)	9,90 €
Kosten je Endgerät Ab 10 Lizenzen: 10% Rabatt Ab 20 Lizenzen: 15% Rabatt	8 € Monatlich

Managed Mobile Device Management

Die Einführung eines unternehmensweiten Mobile Device Managements ist gerade für kleine mittelständische Unternehmen nicht immer sinnvoll. Dabei kann es nur im eigenen Interesse sein, dass Ihre Unternehmensdaten auch auf mobilen Endgeräten geschützt sind.

Häufig ist der Aufwand für die Einführung und Administration jedoch zu hoch. Zudem werden nur in wenigen Fällen die Enterprise-Funktionen großer Lösungen benötigt. Durch das Managed Mobile Device Management haben Sie den optimalen Basisschutz und müssen Sie sich um nichts kümmern. Der Betrieb sowie die Verwaltung des Management-Servers wird in einem hochsicheren regionalen Rechenzentrum durchgeführt. Es werden keinerlei IT-Ressourcen oder IT-Knowhow in Ihrem Hause benötigt.

Mit einem Mobile Device Management schützen Sie das wichtigste Gut Ihres Unternehmens - Ihre Daten!

Security Trainingsplattform

Cybersicherheit so nachhaltig wie nie!

KASPERSKY lab
Gold Partner

Schaffen Sie das Bewusstsein für IT-Sicherheit

Nachhaltiges Cybersecurity Bewusstsein

Egal wie gut die technischen IT-Sicherheitsmaßnahmen auch sind, am Ende sind Ihre Daten nur so sicher, wie das schwächste Glied. Das eigene Personal stellt gerade im Zeitalter von Wirtschaftsspionage und Verschlüsselungstrojanern eine echte Gefahr für die Informationssicherheit dar. Deshalb ist es wichtig, Ihre Mitarbeiter zu sensibilisieren und zu schulen. Häufig wird dafür ein Trainer für einen Tagesworkshop in Anspruch genommen, der dann möglichst viele Mitarbeiter auf einmal sensibilisiert. Das ist jedoch wenig intuitiv und nachhaltig. Informationssicherheit sollte als Prozess integriert werden, genau so sollte auch die Weiterbildung Ihrer Mitarbeiter kontinuierlich stattfinden.

Vielfältige Themen & Micro-Learning

Durch unsere Online Trainingsplattform von Kaspersky erreichen wir eine fortlaufende und nachhaltige Sensibilisierung Ihrer Mitarbeiter. Die Plattform bietet eine Vielzahl intuitiver und leicht zugänglicher Trainingseinheiten und befasst sich mit den folgenden Themenbereichen:

- E-Mail
- Surfen im Internet
- Passwörter
- Soziale Netzwerke
- PC-Sicherheit
- Mobile Geräte
- Vertrauliche Daten
- Persönliche Daten/DSGVO
- Social Engineering
- Sicherheit zu Hause & unterwegs

Der Inhalt beruht auf Simulationen realer Ereignisse unter Hervorhebung der persönlichen Bedeutung der Cybersicherheit für Mitarbeiter. Der Schwerpunkt liegt dabei auf der Vermittlung von Fähigkeiten, nicht lediglich theoretischem Wissen. Daher stehen praktische Übungen und Aufgaben im Mittelpunkt der einzelnen Module. Durch das Micro-Learning-Prinzip (nur 2 bis 10 Minuten je Lerneinheit) wird die Zeit Ihrer Mitarbeiter kaum beansprucht. Außerdem werden so ermüdend lange Lektionen vermieden. Viel mehr steht das regelmäßige und nachhaltige Lernen im Vordergrund. Nach einer erfolgreich absolvierten Trainingseinheit müssen Ihre Mitarbeiter das Gelernte in einem Wissens-Test anwenden. Durch einen automatisch generierten Bericht, werden Ihre Mitarbeiter im wöchentlichen Turnus über ihren aktuellen Trainingsstatus informiert und somit motiviert, die Lerneinheiten weiterhin fortzusetzen.

Individuelles Trainingserlebnis

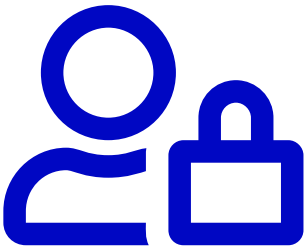
Die Trainingsplattform wird individuell auf Sie und Ihre Mitarbeiter angepasst. Demnach kann der Schutzbedarf unterschiedlicher Mitarbeiter, wie z.B. aus der Produktion oder Buchhaltung, festgelegt werden. Das Trainingsprogramm passt sich dadurch entsprechend den Anforderungen an. Während der Teilnahme wird zudem der Wissensstand der einzelnen Benutzer erkannt und auf Basis dessen das Trainingsprogramm optimal angepasst.

Bereitstellung & regelmäßige Unterstützung

Die IT Südwestfalen AG unterstützt Sie bei der Inbetriebnahme der Plattform. In einem Kickoff-Termin werden der Status sowie die Ziele Ihres Unternehmens mit der Trainingsplattform besprochen und erarbeitet. Anschließend erfolgt die Einrichtung und Konfiguration der Plattform. Ihr Administrator erhält eine entsprechende Einweisung in das System um als Ansprechpartner Ihrer Mitarbeiter fungieren zu können.

Auf Wunsch übernimmt die IT Südwestfalen AG im Zuge des Paketes Standard die gesamte Administration der Plattform und entlastet so Ihren Administrator. Das betrifft sowohl die Konfiguration bestehender und neuer Benutzer als auch die Überprüfung der einzelnen Lernfortschritte. Ergebnisse werden in einem individuellen Quartalsbericht persönlich vorgestellt, um den maximalen Nutzen für Ihr Unternehmen zu erzielen. Zudem unterstützen wir Sie vor Inbetriebnahme der Plattform bei der Ermittlung des Schutzbedarfes der Teilnehmer.

Vertrauen Sie Ihrem IT-Sicherheitsexperten der Region!



"Durch das Micro-Learning-Prinzip, wird die Zeit Ihrer Mitarbeiter kaum beansprucht"

Security Trainingsplattform

	Basic	Standard
Umfangreiche Online Trainingsplattform	✓	✓
Universeller mehrstufiger Schulungsplan mit über 450 Fertigkeiten, für Anfänger bis hin zu Fortgeschrittenen	✓	✓
Kontinuierliche Schulung durch Micro-Learning	✓	✓
Geeignet für PC & Smartphone	✓	✓
Betrieb als Cloud-Dienst in einem Rechenzentrum	✓	✓
Automatisierte Berichte zum aktuellen Status	✓	✓
Einfache Inbetriebnahme (Kickoff-Termin, Bereitstellung der Plattform, Einweisung des Administrators)	✓	✓
Erweiterte Inbetriebnahme (zus. zur einfachen Inbetriebnahme: Konfiguration der Plattform, Unterstützung bei Ermittlung des Schutzbedarfs, Einweisung der Teilnehmer)	✗	✓
Administration der Plattform durch die IT Südwestfalen AG	✗	✓
Individuelle Quartalsberichte inkl. persönlicher Vorstellung	✗	✓
Stundensatz für weitere Arbeiten & individuelle Sicherheitsfragen zu den Inhalten der Plattform (nach Aufwand)	150 €	120 €
Einmalige Bereitstellungsgebühr	990 €	990 €
Kosten je Benutzer Laufzeit: 24 Monate Mindestabnahme 5 Benutzer Ab 10 Benutzer: 10% Rabatt Ab 20 Benutzer: 20% Rabatt Ab 50 Benutzer: 30% Rabatt	12 € Monatlich	18 € Monatlich

"Nachhaltige Sensibilisierung Ihrer Mitarbeiter- der optimale Schutz vor IT-Sicherheits-Bedrohungen"

Security Awareness der neusten Generation

Datenschutz

Jetzt EU-DSGVO ready werden

IT-Sicherheit
- Informationssicherheit
- Datensicherung
- Virenschutz
- Firewalling
- Mobile Device Management
- Security Trainingsplattform
- Datenschutz

Bereiten Sie Ihr Unternehmen optimal auf die EU-DSGVO vor

Was ist die EU-Datenschutz-Grundverordnung?

Die EU-DSGVO dient zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Sie bezieht sich auf personenbezogene und personenbeziehbare Daten. Die Verordnung trat am 25.05.2016 in Kraft und die Übergangszeit endete am 25.05.2018.

Jedes Unternehmen, ab 9 Mitarbeitern bei automatisierter und ab 20 Mitarbeitern bei genereller Verarbeitung personenbezogener Daten, benötigt einen Datenschutzbeauftragten. Dieser soll dem Landesamt für Informationssicherheit NRW bis zum 25.05.2018 gemeldet werden. Sie haben entweder die Möglichkeit einen eigenen Mitarbeiter zum internen oder einen Dienstleister zum externen Datenschutzbeauftragten zu ernennen. Benennt man einen eigenen Mitarbeiter als Datenschutzbeauftragten genießt dieser einen besonderen Kündigungsschutz. Darüber hinaus darf die Bestellung des Mitarbeiters zum Datenschutzbeauftragten ohne sachlichen Grund nicht entzogen werden, wobei der Wille auf einen externen Datenschutzbeauftragten zu wechseln keinen sachlichen Grund zur Abberufung darstellt. Ein Datenschutzbeauftragter muss zuverlässig sein und über die entsprechenden Fachkenntnisse verfügen. Es darf keine Kollision mit den betrieblichen Aufgaben bestehen. Ein IT Administrator darf diese Aufgabe beispielsweise nicht erfüllen.

Individuelle Unterstützung

Das Datenschutz Basispaket hilft Ihnen dabei die Mindestvoraussetzungen der EU-DSGVO zu erfüllen. Neben einem Workshop, der Ihnen die Struktur der Verordnung sowie Ihre Rechte und Pflichten aufzeigt, erhalten Sie das Wissen darüber das benötigte Verzeichnis für Verarbeitungstätigkeiten zu erstellen. Anschließend können Sie einen Mitarbeiter der IT Südwestfalen AG zu Ihrem externen Datenschutzbeauftragten benennen.

Durch Handlungsempfehlungen und Bestpractices erhalten Sie zudem Empfehlungen für Ihr Unternehmen. Dieses Basispaket lässt sich nach Belieben erweitern. Auf Wunsch werden Ihnen zum Beispiel eine individuelle und EU-DSGVO kompatible Datenschutzerklärung für Ihre Website erstellt oder ein nach VDS auf Sie abgestimmtes EU-DSGVO Quick Audit durchgeführt. Diese Optionen helfen Ihnen nicht nur der Verordnung zu entsprechen, sondern das Thema Datenschutz aktiv anzugehen und zu leben, um Kunden-, Lieferanten- und Mitarbeiterdaten bestmöglich zu schützen.

Datenschutzpaket

	Basic
Workshop zur Struktur der EU-DSGVO	✓
Workshop zum Verzeichnis der Verarbeitungstätigkeiten	✓
Aufklärung über Rechte und Pflichten	✓
Handlungsempfehlungen zur Umsetzung der EU-DSGVO	✓
Ernennung eines Mitarbeiters der IT Südwestfalen AG zum externen Datenschutzbeauftragten bis 31.12.19 (Die Ernennung für ein weiteres Jahr kostet pauschal 500 €)	✓
Mitteilung über rechtliche Updates der EU-DSGVO bis 31.12.19	✓
Stundensatz für weitere Arbeiten (nach Aufwand)	150 €
Kosten	1.500 € Einmalig

Optionen

Individuelle Datenschutzerklärung auf Website (kein eCommerce) — 300 € Einmalig
- Erstellung einer EU-DSGVO entsprechenden Datenschutzerklärung für Ihre Internetseite

EU-DSGVO Quick Audit — 1.200 € Einmalig
- Durchführung des Quick-Audits mit 26 Fragen
- Dokumentation & Handlungsempfehlungen
- Besprechung der Ergebnisse

Individueller Workshop zur Mitarbeitersensibilisierung — 150 € je Stunde
- Erarbeitung und Durchführung eines individuellen Workshops zur optimalen Sensibilisierung Ihrer Mitarbeiter für den Datenschutz
- Berechnung nach Aufwand, bei Buchung des Datenschutzpaketes reduziert sich der Stundensatz auf 120 € je Stunde

Datenschutz ist uns und Ihnen wichtig!

Angebote nur für Gewerbetreibende. Preise zzgl. gesetzlicher MwSt.