einsnulleins
IT. Läuft.



einsnulleins Leistungsbeschreibung

STAND: 10/2026

Unsere Leistungsbeschreibungen 2

1. Ein erster Überblick 2

2. Im Detail: IT. Läuft. Paket 3

2.1 Voraussetzungen für alle IT. Läuft. Pakete 4

2.2 Desktop und Server Management 4

2.3 Firewall Management 6

2.4 Microsoft 365 Management - die zentrale Verwaltung von Microsoft 365 8

2.5 Passwort Management - die zentrale und sichere Verwaltung Ihrer Passwortdatenbank 9

2.6 Network Attached Storage (NAS) Management 11

2.7 Switch Management 12

2.8 Fernwartung 13

2.9 Störungsbeseitigungen - wir regeln das 13

2.10 Umfassende Administrationstätigkeiten 14

2.11 Koordination externer Dienstleister 14

2.12 Unsere Servicezeiten 14

2.13 Nicht enthaltene Leistungen 15

3. IT. Läuft. Plus Paket 16

3.1 Active Directory und Entra ID Sicherheitsmanagement 16

3.2 Digitale Lernplattform inklusive IT-Sicherheitsschulungen 17

3.3 IT-Sicherheitsberatung für Geschäftsleitungen 18

4. IT. Läuft. Premium Paket 18

Unsere Leistungsbeschreibungen

IT ist kompliziert, die Betreuung der IT deswegen auch. Für alle, die genau wissen wollen, zu welchen Leistungsumfängen wir uns verpflichten und was nicht von unseren Verträgen umfasst ist, geben wir im Folgenden einen detaillierten Einblick.

1. Ein erster Überblick

Unsere laufende IT-Betreuung bieten wir in drei Paketen an:

IT. Läuft. Paket	**IT. Läuft. Plus Paket**	**IT. Läuft. Premium Paket**
Betreuung der kompletten IT-Infrastruktur bestehend aus: • Desktop Management • Server Management • Monitoring • automatische Installation wichtiger Updates • Anti-Virus Management • Firewall Management • Microsoft 365 Management • Management E-Mail Archivierung • Passwort Management • NAS Management • Switch Management • kostenloser telefonischer Support bei Problemen • Beseitigung aller Störungen, die durch Fernwartung behoben werden können • umfassende Administratoren-Tätigkeiten • Koordination externer Dienstleister	IT. Läuft. Paket erweitert um: • Active Directory und Entra ID Security Management • E-Learning-Plattform mit IT-Security-Schulungen für jeden Mitarbeiter • zwei Phishing-Kampagnen pro Jahr • halbjährliches Security-Gespräch mit Umsetzungs- und Maßnahmenplan	IT. Läuft. Plus Paket erweitert um: • Störungsbeseitigung auch vor Ort • quartärliches Security-Gespräch mit Umsetzungs- und Maßnahmenplan • Beratung / Consulting, insbesondere bei der Weiterentwicklung der IT-Security- und IT-Infrastruktur und Begleitung der strategischen Entwicklung Ihres Unternehmens

Zusätzlich bieten wir folgende Module an
Die IT-Infrastrukturen unserer Kunden sind sehr vielfältig. Damit Sie nichts zahlen, was Sie gar nicht benötigen, können Sie bei uns noch zusätzlich folgende Leistungen buchen:

- E-Mail Archivierung
- Mobile Device Management
- Software Lizenzen

2. Im Detail: IT. Läuft. Paket

Hier werden Ihre Systeme von uns überwacht, wichtige Updates automatisch installiert und wir sorgen für Virenschutz. Durch die kontinuierliche Überwachung der Geräte können mögliche Risiken erkannt und behoben werden, bevor es zu Problemen kommt. Sie bekommen von uns entsprechende Hinweise, wenn wir Handlungsbedarf sehen.

Damit haben Sie eine wichtige Basis für einen sicheren und störungsfreien IT-Betrieb.

Dieses Paket umfasst außerdem

- kostenlosen telefonischen Support bei Problemen,
- die kostenlose Störungsbeseitigung per Fernwartung
- und umfassende administrative Tätigkeiten.

Diese Leistungen bieten wir Ihnen zum monatlichen Festpreis an. Damit ist es unser Problem, wenn wir für die Lösung anfallender Probleme auch mal länger brauchen. Da sämtliche Aufwände zu unseren Lasten gehen, haben wir ein maximales Interesse daran, Probleme schnell und nachhaltig zu lösen.

Unsere Leistungen beziehen sich im Wesentlichen auf das Betriebssystem und Standardsoftware-Produkte wie Office, Google, PDF-Reader oder Browser, die auf dem Desktop bzw. Server installiert sind. Für darüber hinaus explizit benannte Anwendungsprogramme kümmern wir uns in der jeweils vom Hersteller angebotenen, aktuellsten Version ebenfalls um alle Probleme. Bei der übrigen Software unterstützen wir Sie mindestens durch die Koordination Ihrer Anfragen gegenüber den Anbietern.

Es hat in der Vergangenheit sehr wenige Fälle gegeben, bei denen durch unzureichenden Ausbildungsstand der Nutzer oder stark von der Norm abweichendem Nutzungsverhalten Aufwände entstanden sind, die es uns unmöglich machten, langfristig wirtschaftlich zu arbeiten. In diesen Ausnahmefällen melden wir uns und schlagen entweder geeignete Maßnahmen vor oder sprechen mit Ihnen über eine Preisanpassung.

2.1 Voraussetzungen für alle IT. Läuft. Pakete

Um die Sicherheit und Stabilität Ihrer IT-Infrastruktur gemäß aktuellen Best Practices (u.a. BSI, Microsoft) zu gewährleisten, sind folgende Voraussetzungen zwingend erforderlich:

1. **Endpoint Security (Antivirenschutz)**
    a. Für alle Geräte muss eine aktuelle und funktionierende Endpoint Security vorhanden sein.
    b. Diese ist in allen IT.Läuft.-Paketen bereits enthalten.
2. **Backup-Strategie**
    a. Regelmäßige Sicherung aller wichtigen Systeme:
        i. **Vor-Ort**: Backup für Server und virtuelle Maschinen.
        ii. **Cloud-Systeme**: Backup für alle in der Cloud betriebenen Systeme.
        iii. **Microsoft 365 Umgebung**: vollständiges Backup
    b. Falls die passende Backup-Lösung nicht vorhanden ist, erstellen wir ein separates Angebot.
3. **Multi-Faktor-Authentifizierung (MFA)**
    a. Für alle wichtigen Accounts ist MFA zwingend erforderlich.
    b. Falls keine Lösung vorhanden ist, unterbreiten wir Ihnen ein passgenaues Angebot.

Nachfolgend erfahren Sie die Details unserer Leistungen.

2.2 Desktop und Server Management

Monitoring - wir haben alles im Blick

Sowohl Server als auch Workstations werden von uns rund um die Uhr mit einem agentenbasierten, automatischen Software-Programm hinsichtlich der Lauffähigkeit der wichtigsten Windows-Dienste, Überschreitung eines Schwellenwertes des noch verfügbaren Festplattenspeichers, Aktualität der Anti-Virus-Signaturen, Prüfung auf kritische Ereignisse in den Windows-Ereignisprotokollen und physischen Festplattenzustand überwacht. Dies gilt natürlich nur für die Hard- und Software-komponenten, welche uns diese Information bereitstellen. Wir informieren Sie selbstverständlich immer dann, wenn für uns oder Sie kritische Informationen nicht zur Verfügung stehen.

Installation aktueller Sicherheitsupdates - immer auf dem neuesten Stand

Installation der vom Hersteller als „kritisch“ oder „wichtig“ eingestuften Microsoft- Betriebssystemupdates sowie Updates für Standardprogramme verschiedenster Anbieter. Eine vollständige Liste der unterstützten Programme kann auf der Seite des Herstellers der von uns eingesetzten Lösung eingesehen werden.

Diese automatisierten Sicherheitsupdates werden ausschließlich für Windows-Betriebssysteme durchgeführt. Linux und Apple Betriebssysteme sind von der Automatisierung ausgeschlossen, Sicherheitsupdates werden lediglich anlassbezogen manuell ausgeführt.

Die zentrale Überwachung und Freigabe der Updates erfolgt durch unsere ausgebildeten Techniker. Wir gehen natürlich auf Nummer sicher und führen eine tägliche Abfrage der erfolgreichen Installation durch.

Nach Installation eines Updates ist oftmals ein Neustart erforderlich, den Sie selbst durchführen können. Danach sind Sie wieder direkt startklar und arbeitsfähig.
Sie sind damit einverstanden, dass die vom Softwarehersteller als „kritisch“ oder „wichtig“ eingestuften Sicherheitsvorkehrungen automatisch ohne vorherige Prüfung auf den Systemen installiert werden, um Sicherheitslücken zu schließen oder Fehler zu beheben.

Die Verantwortung für die Fehlerfreiheit der Sicherheitsupdates, die Sinnhaftigkeit der Risiko-Klassifizierung sowie die Kompatibilitätseinschätzung mit der zu aktualisierenden Software liegt allein beim jeweiligen Softwarehersteller.

Ihnen ist bewusst, dass Sicherheitsaktualisierungen Veränderungen an der installierten Software vornehmen, um die Sicherheit zu erhöhen. Bei diesen Veränderungen kann es zu Problemen kommen, die die Lauffähigkeit des Systems negativ beeinflussen. Für Folgeschäden aus diesem Umstand übernehmen wir keine Verantwortung. Aber wir lassen Sie nicht im Stich und übernehmen für Sie selbstverständlich die Problemlösung nach üblichen Standards.

Backup-Policy

Mit Verabschiedung einer Backup-Policy (Richtlinie für Sicherheitskopien) legen wir den Grundstein für eine funktionierende Datensicherung. Unsere Techniker arbeiten dabei nach den jeweils geltenden technischen Normen. Dabei tun wir alles in unserer Macht stehende, um eine aktuelle und angemessene Datensicherung in geeigneter Form zu betreiben und alle Voraussetzungen für eine wirtschaftlich vernünftige Wiederherstellung von verloren gegangenen Daten schaffen zu können. Insbesondere bei Neueinrichtungen und vor Beginn von Wartungs- und Reparaturarbeiten werden wir in Abstimmung mit Ihnen eine Datensicherung durchführen.

Solange keine Backup-Policy vorliegt, tragen Sie die Verantwortung für die Datensicherung.

Daran anschließend müssen Sie angemessene und dem Stand der Technik entsprechende Schutzmaßnahmen treffen, um eine Beeinträchtigung von Daten durch Computerviren oder ähnliche Phänomene, die eine Unbrauchbarmachung von Daten herbeiführen, zu verhindern. Hierzu werden wir Sie auf entsprechende Maßnahmen hinweisen und diese - Ihre Beauftragung vorausgesetzt - auch umsetzen.

Wir kümmern uns bei den im Rahmen der Backup Policy dokumentierten Systemen um eine Wiederherstellung des letzten, lauffähigen Zustandes. Wir weisen Sie darauf hin, dass es aufgrund der Tatsache, dass dieser Stand etwas weiter zurückliegen kann, zu Datenverlusten kommen kann. Wenn darüber hinaus Daten aus nicht lauffähigen Backups oder Anwenderdaten granular wiederhergestellt werden sollen, ist dies eine kostenpflichtige Leistung und muss gesondert beauftragt werden.

Anti-Virus Management - Sicherheit geht vor

Das Anti-Virus Management bietet Ihnen einen bestmöglichen Schutz für Ihr Gerät bzw. Ihren Server. Die Leistung umfasst die Bereitstellung von Lizenzen inklusive Wartungs-/Update-Pakete durch uns für Ihren Arbeitsplatz- bzw. Server-Schutz.

Unser Anti-Virus Management kümmert sich automatisch um die Überprüfung, ob bei Ihnen ein aktueller Virenscanner im Einsatz ist. Beide Beteiligten vereinbaren, dass eine Alarmierung erfolgt, sobald eine Signatur älter als 5 Tage sein sollte.

Auch wenn wir unser Bestmögliches unternehmen, können auch wir leider keinen 100%igen Anti-Virus-Schutz bieten. Wir werden nach den üblichen Standards Maßnahmen zum Schutz Ihrer Arbeitsplätze und Server durchführen und überprüfen.

Zusammenfassender Report - alles im Blick

Wenn Sie wünschen, können wir Ihnen eine Zusammenfassung erstellen, die Ihnen einen Überblick über die installierte Software pro Gerät verschafft. Ebenso können Sie von uns einen Report über Ihr Inventar bzgl. Ihrer installierten Hardwarekomponenten erhalten.

Bereinigung von temporären Dateien und Ereignisprotokollen - Ordnung muss sein

Eine regelmäßige Leerung von gespeicherten Daten ist für den ordnungsgemäßen Betrieb eines Arbeitsplatzes oder eines Servers essentiell, sodass eine anlassbezogene Bereinigung von temporären Dateien, des Browser-Speichers, des Terminalserver-Speichers und von Ereigniseinträgen vorgenommen wird.

Zusätzliche Leistungen des Server Managements

Neben den oben genannten Leistungen führen wir auf Servern folgende Tätigkeiten durch:

Die Server werden täglich auf erfolglose Anmeldeversuche geprüft. Zudem unterstützen wir Sie bei der Überprüfung der Server- bzw. Prozessor-Temperatur. Des Weiteren führen wir eine Leistungsüberwachung Ihrer Server hinsichtlich Prozessorauslastung, Speichernutzung, Festplattenleistung und Netzwerkkarten-Auslastung durch.

Nach Installation eines Updates ist oftmals ein Neustart erforderlich, den Sie selbst durchführen können. Alternativ vereinbaren wir mit Ihnen feste Termine, zu denen wir uns um den Neustart der Systeme kümmern. Selbstverständlich werden Sie unabhängig davon, falls vereinbart, im Vorfeld über eine geplante Installation von Updates informiert. Im Anschluss daran sind Sie wieder direkt startklar und arbeitsfähig.

2.3 Firewall Management

Unternehmensnetzwerke sind ein regelmäßiges Ziel von Angriffen. Eine Firewall bietet Schutz vor unbefugten Zugriffen und soll darüber hinaus Gefahren vom Unternehmen abhalten, die Arbeitsfähigkeit

durch Lastverteilung des Datenverkehrs sicherstellen, Aufrufe von gefährlichen oder illegalen Webseiten unterbinden sowie eine sichere Anbindung von Außenstellen und Heimarbeitsplätzen gewährleisten. Zudem bietet sie die Möglichkeit, Netzwerke in logisch getrennte Einheiten zu trennen.

Die einmalige Einrichtung einer Firewall genügt nicht, um ein Unternehmen dauerhaft vor Angriffen von außen zu schützen. Aufgrund der nahezu täglichen Änderung der Gefahrenlage und der Anforderungen des Unternehmens ist es zwingend erforderlich, die Konfiguration einer Firewall ständig anzupassen.

Enthaltene Leistungen

Automatische Aktualisierung – immer auf der sicheren Seite

Der komplette Netzwerkverkehr wird durch die Firewall an einem zentralen Punkt gefiltert. Damit Schadsoftware erkannt und Angriffe identifiziert werden können, müssen die Virensignaturen sowie Spam- und Content-Filter regelmäßig aktualisiert werden. Die Verantwortung für die Fehlerfreiheit der Filter und Signaturen sowie die Sinnhaftigkeit der Risiko-Klassifizierung liegt allein beim jeweiligen Content-Lieferanten.

Automatische Sicherung der Konfiguration

Wir sichern automatisch die Konfiguration der Firewall. Dies ermöglicht eine unmittelbare Wiederherstellung des Systems im Bedarfsfall, beispielsweise bei einem Hardwaredefekt oder Konfigurationsfehlern.

Monitoring der Firewall

Wir überprüfen Ihre Firewall und können dadurch Probleme schneller erkennen und lösen.

Einrichtung von VPN-Zugriffen

Auf Wunsch übernehmen wir die Einrichtung von verschlüsselten Netzwerkzugriffen für Mitarbeiter mit Heimarbeitsplätzen oder im Außendienst.

Regelmäßige Aktualisierung der Firmware - immer funktionsfähig bleiben

Wir nehmen regelmäßig Aktualisierungen der Firewall-Firmware mit aktuellen Updates vor, um Ihr System immer auf dem aktuellsten Stand zu halten.

Fehleranalyse und -behebung

Sofern technische Probleme an der Firewall auftreten, kümmern wir uns um eine umfangreiche Analyse und gleichzeitige Behebung des Fehlers, sodass Ihr Unternehmen wieder vollständig geschützt ist.

Nicht enthaltene Leistungen

Beseitigung der Folgen von Angriffen

Die Leistung umfasst nicht die Beseitigung eines Virenbefalls oder die Folgen eines Angriffes auf Ihr Unternehmensnetzwerk. Jedoch lassen wir Sie natürlich auch hier nicht im Stich und stehen Ihnen bei Problemen dieser Art jederzeit zur Verfügung. Die hier anfallenden Tätigkeiten werden separat abgerechnet.

2.4 Microsoft 365 Management - die zentrale Verwaltung von Microsoft 365

Microsoft 365 Pakete bzw. Pläne bieten eine Kombination bestehend aus verschiedenen Online-Diensten, Office-Webanwendungen und lokal installierbarer Office-Software. Damit alle Anwendungen reibungslos ineinandergreifen und der Aufwand in der Konfiguration und Wartung der Produkte minimal ist, stellen wir Ihnen ausgewählte Microsoft 365-Pläne als Managed Service zur Verfügung.

Hierin sind alle Arbeiten über die Microsoft 365 Administrationsoberfläche enthalten.

Wir kümmern uns um alle Störungen im Zusammenhang mit der zentralen Verwaltung von Microsoft 365. Für Sie entstehen für die Bereitstellung neuer Lizenzen, Änderungen und Kündigungen keine zusätzlichen Verwaltungskosten. Nicht enthalten sind die Lizenzkosten bei Microsoft. Die werden gesondert berechnet.

Enthaltene Leistungen

Auswahl der passenden Lizenzen

Wir beraten Sie bei der Auswahl des für Sie passenden Microsoft 365 Produktes bzw. Planes. Dabei werden neben den aktuellen Anforderungen nach Möglichkeit auch zukünftige Nutzungsszenarien berücksichtigt.

Bereitstellung der Lizenzen

Wir kümmern uns um die technische Bereitstellung der separat zu buchenden, kostenpflichtigen Lizenzen in Ihrer Microsoft 365 Umgebung. Zu viel bereitgestellte Lizenzen werden wir in Abstimmung mit Ihnen entfernen.

Automatische Verlängerung der Lizenzen - wir übernehmen

Die monatlich bzw. jährlich gebuchten Pakete bzw. Pläne verlängern sich automatisch, so dass Sie dauerhaft arbeitsfähig bleiben.

Umzug der zentralen Verwaltung

Wir unterstützen Sie bei Bedarf beim Umzug einer bereits vorhandenen Microsoft 365 Verwaltung in die Zuständigkeit von uns. Dafür entstehen Ihnen keine zusätzlichen Kosten.
Sofern noch keine Verwaltung existiert und diese neu eingerichtet werden muss, wird der damit verbundene Leistungsumfang von uns gesondert angeboten und zur Abrechnung gebracht.

Administrationstätigkeiten

- Bereitstellung von Informationen über die aktuell vorliegende Konfiguration
- Anlage und Pflege von User-Accounts und Lizenzen
- Anlage eines individuellen Admin-Accounts für Sie
- Eingliederung neuer Mitarbeiter
- Zurücksetzen eines Passwortes (bspw. nach Ablauf, bei Verlust)
- Gruppen- und Rechteverwaltung
- Einrichtung von freigegebenen Sammel-Postfächern & Verteilergruppen
- Ausgliederung ehemaliger Mitarbeiter
- Verwaltung und Aktualisierung der über Microsoft Intune (MDM) verteilten Softwarepakete

Störungsbeseitigungen

- Probleme bei der Anmeldung am Microsoft 365 Account
- Probleme in Microsoft Office (Word, Excel, PowerPoint etc.)
- Probleme beim Zugriff und der Nutzung der Web-Versionen/Online-Apps (Word, Excel, PowerPoint, Outlook etc.)
- Probleme bei der E-Mail-Kommunikation
- Probleme bei der Verwendung von Microsoft Teams
- Probleme bei der Verwendung von Microsoft Intune (MDM)

Auch bei Problemen, die ggf. die Unterstützung von Microsoft selbst erfordern, helfen wir weiter. Dazu zählt insbesondere:

- Meldung von Problemen an den Microsoft Support
- Begleitung der Problemlösung durch den Microsoft Support
- Kommunikation von Statusinformationen von Ihnen bzw. des Microsoft Supports

Die Lösung der Probleme obliegt hierbei dem Microsoft Support selbst.

2.5 Passwort Management - die zentrale und sichere Verwaltung Ihrer Passwortdatenbank

Schützen Sie Ihr Unternehmen gegen Datendiebstahl mit unserem hochsicheren Passwortmanager Keeper.

Keeper schützt die Passwörter Ihrer Organisation mit einem hochsicheren und unkomplizierten Passworttresor. Damit der Passwortmanager perfekt auf Ihre Bedürfnisse zugeschnitten ist und der Aufwand in der Konfiguration und Wartung der Produkte minimal ist, stellen wir Ihnen ausgewählte Keeper-Pläne als Managed Service zur Verfügung.

Dabei wird die komplette Verwaltung der Keeper Umgebung von uns übernommen. Im Rahmen des Managed Service Ansatzes übernehmen wir die folgenden Leistungen:

Auswahl der passenden Lizenzen

Wir beraten Sie bei der Auswahl des für Sie passenden Keeper Produktes bzw. Planes. Dabei werden neben den aktuellen Anforderungen nach Möglichkeit auch zukünftige Nutzungsszenarien berücksichtigt.

Bereitstellung der Lizenzen

Wir kümmern uns um die technische Bereitstellung der separat zu buchenden, kostenpflichtigen Lizenzen in Ihrer Keeper Umgebung. Zuviel bereitgestellte Lizenzen werden wir in Abstimmung mit Ihnen entfernen. Für Sie entstehen für die Bereitstellung neuer Lizenzen, Änderungen und Kündigungen keine zusätzlichen Verwaltungskosten.

Automatische Verlängerung der Lizenzen

Die monatlich bzw. jährlich gebuchten Pakete bzw. Pläne verlängern sich automatisch, so dass Sie dauerhaft arbeitsfähig bleiben.

Störungsbeseitigungen

- Probleme bei der Anmeldung am Keeper Account
- Probleme bei der Single-Sign-On Integration oder der Active Directory bzw. LDAP-Synchronisierung
- Probleme bei der Freigabe von Passwörtern
- Probleme bei der Verwendung der Keeper Browser-Erweiterung, Desktop App oder dem Web-Tresor
- Probleme bei Berechtigungen von Datensätzen

Auch bei Problemen, die ggf. die Zuarbeit von Keeper selbst bedingen, helfen wir weiter. Dazu zählt insbesondere:

- Meldung und Begleitung von Problemen an den Hersteller-Support
- Kommunikation von Statusinformationen von Ihnen bzw. des Hersteller Supports

Die Lösung der Probleme obliegt hierbei dem Keeper Support.

Administrationstätigkeiten

- Bereitstellung von Informationen über die aktuell vorliegende Konfiguration
- Anlage und Pflege von User-Accounts und Lizenzen
- Eingliederung neuer Mitarbeiter
- Zurücksetzen eines Accounts durch Tresorübertragung (bspw. nach Ablauf oder bei Verlust)
- Teams- und Rechteverwaltung
- Anlage eines individuellen Admin-Accounts für Sie
- Ausgliederung ehemaliger Mitarbeiter

Darüber hinaus übernehmen wir optional und gegen Aufpreis die folgenden Leistungen:

- Nachträgliche Einrichtung einer Single-Sign-On Lösung
- Nachträgliche Einrichtung von Active Directory oder LDAP-Synchronisierung
- Durchführung von Produktschulungen
- Nachträgliche Migration bereits bestehender Passwörter aus anderen Passwortmanagern

2.6 Network Attached Storage (NAS) Management

Allgemeine Informationen

Ein NAS dient nicht nur als zentrale Ablage für Dateien und Daten, um das gemeinsame Arbeiten an Dokumenten zu erleichtern, unternehmenskritische Dateien aufzubewahren oder virtuelle Maschinen von dort zu starten. Ein NAS ist sehr häufig auch Ziel der Datensicherung von Server-Systemen und elementarer Bestandteil einer Backup-Strategie zur Vermeidung von Datenverlusten. Vor diesem Hintergrund ist es wichtig, ein im Netzwerk eines Unternehmens befindliches NAS ähnlich wie z.B. ein Serversystem im Rahmen der laufenden Betreuung zu überwachen und regelmäßig zu aktualisieren.

Ziel des NAS Managements

Es reicht nicht aus, ein NAS einmalig einzurichten. Um den Zugriff auf Daten dauerhaft gewährleisten zu können und Unternehmen kontinuierlich gegen Datenverlust zu schützen, ist es wichtig, ein NAS fortlaufend zu betreuen. Aufgrund von Software- und Sicherheitsupdates des NAS-Herstellers und der kontinuierlichen Weiterentwicklung Ihrer IT-Umgebung, ist eine ständige Pflege der Konfiguration des NAS unerlässlich. So gilt es beispielsweise, den Zustand des Systems regelmäßig zu überprüfen und die Speichergröße des NAS bei Bedarf zu erweitern.

Aktualisierung der Firmware

Die Software des NAS wird herstellerseitig stetig verbessert. Änderungen und Erweiterungen werden regelmäßig in Form von Updates der Firmware bereitgestellt. Die neueste Versionen schließen dabei nicht nur bekannte Sicherheitslücken, sie bringen in aller Regel auch Features mit sich, die nach vorheriger Prüfung freigegeben werden können. Aktualisierungen der Firmware sollten daher bei jedem NAS zeitnah eingespielt werden.

Monitoring des NAS

Durch eine stetige Überprüfung der wichtigsten Parameter können Probleme proaktiv erkannt und gelöst werden. Dies macht sich vor allem dann bemerkbar, wenn das NAS nach einem Stromausfall nicht wieder hochfährt oder aus anderen, nicht vorhersehbaren Gründen die Verbindung zum Netzwerk verliert. Eine weitere Fehlerquelle ist der Ausfall einzelner Festplatten, welche durch ein Monitoring frühzeitig erkannt werden können.

Einrichtung von Benutzerkonten auf dem NAS

Auf Wunsch übernehmen wir die Einrichtung von individuellen Benutzerkonten, um sich einen eigenen direkten Zugriff auf das NAS zu verschaffen oder binden das NAS an eine vorhandene Verzeichnisstruktur (z.B. Active Directory) an.

Alle Leistungsmerkmale auf einen Blick:

- Monitoring der Erreichbarkeit des NAS
- Überwachung des Zustandes der in dem NAS verbauten Festplatten
- Monitoring wichtiger Systemparameter (z.B. verfügbarer Speicherplatz, CPU-Auslastung, Temperatur)
- regelmäßige Aktualisierung der Firmware
- Übernahme des User- und Berechtigungsmanagements
- Fehleranalyse und -behebung (exkl. Hardware & exkl. Datenwiederherstellung)

Die Wiederherstellung von Daten, die für eine Reparatur ggf. benötigten Ersatzteile sowie die Reparatur durch einen Techniker vor Ort sind im Leistungsumfang des NAS Managements nicht enthalten und werden separat abgerechnet. Das NAS Management deckt ebenfalls keine Datenverluste aufgrund von nicht ordnungsgemäß gesicherten Daten und dessen Folgen ab.

2.7 Switch Management

Allgemeine Informationen

Switche sind wesentlicher Bestandteil eines Netzwerks. Sie verbinden mehrere Geräte innerhalb eines Netzwerkes, z.B. Computer, Access Points oder Drucker miteinander. Mit Hilfe eines Switches können diese Geräte Informationen teilen und untereinander kommunizieren. Vor diesem Hintergrund ist es wichtig, einen im Netzwerk eines Unternehmens befindlichen Switch, ähnlich wie z.B. ein Serversystem, im Rahmen der laufenden Betreuung zu überwachen und regelmäßig zu aktualisieren.

Ziel des Switch Managements

Es reicht nicht aus, einen Switch einmalig einzurichten. Um reibungslose Kommunikation der Geräte innerhalb eines Netzwerks dauerhaft sicherzustellen, ist es wichtig einen Switch fortlaufend zu betreuen. Aufgrund von Software- und Sicherheitsupdates des Switch-Herstellers und der kontinuierlichen Weiterentwicklung Ihrer IT-Umgebung, ist eine ständige Pflege der Konfiguration des Switches unerlässlich. So gilt es beispielsweise, den Zustand des Systems regelmäßig zu überprüfen.

Aktualisierung der Firmware

Die Software des Switches wird herstellerseitig stetig verbessert. Änderungen und Erweiterungen werden regelmäßig in Form von Updates der Firmware bereitgestellt. Die neuesten Versionen schließen dabei nicht nur bekannte Sicherheitslücken, sie bringen in aller Regel auch Features mit sich, die nach vorheriger Prüfung freigegeben werden können. Aktualisierungen der Firmware sollten daher bei jedem Switch zeitnah eingespielt werden.

Monitoring des Switches

Durch eine stetige Überprüfung der wichtigsten Parameter können Probleme proaktiv erkannt und gelöst werden.

(Um-)Konfiguration des Switches

Auf Wunsch übernehmen wir die Einrichtung, Umkonfiguration und Freigabe von Ports, VLANs und PoE-Einstellungen.

Alle Leistungsmerkmale auf einen Blick:

- Monitoring der Erreichbarkeit des Switches
- Monitoring wichtiger Systemparameter
- regelmäßige Aktualisierung der Firmware
- Fehleranalyse und -behebung (exkl. Hardware & exkl. Datenwiederherstellung)

Die für eine Reparatur ggf. benötigten Ersatzteile sowie die Reparatur durch einen Techniker vor Ort sind im Leistungsumfang des Switch Managements nicht enthalten und werden separat abgerechnet.

2.8 Fernwartung

Wir versuchen so viel wie möglich mit Fernwartung zu erledigen. Das spart Kosten, Zeit und schont die Umwelt.

Unsere Fernwartung ermöglicht für Sie eine direkte Problemlösung durch unsere Techniker aus der Ferne über eine nach dem üblichen Standard gesicherte Internetverbindung. Ihre Maus und Tastatur können dabei aus der Ferne gesteuert werden. Dazu benötigen wir natürlich zunächst Ihr Einverständnis darüber, dass wir Zugriff auf die Systemeinstellungen und sämtliche Daten haben dürfen. Aber keine Sorge! Jeder Mitarbeiter behandelt Ihre Daten mit hoher Sorgfalt, denn dazu sind wir verpflichtet.

2.9 Störungsbeseitigungen - wir regeln das

- Probleme bei der Anmeldung am System / an der Domäne
- Probleme mit dem gesicherten Zugriff auf das interne Netzwerk (VPN)
- Probleme mit dem Betriebssystem im Allgemeinen
- Probleme mit betriebssystemintegrierten Diensten (bspw. Active Directory, DNS, DHCP, File/Print…)
- Probleme in Microsoft Office (Word, Excel, PowerPoint etc.)
- Probleme bei der E-Mail Kommunikation
- Probleme mit PDF Reader Software (Adobe PDF Reader etc.)
- Probleme mit dem Browser (Microsoft Edge, Google Chrome, Mozilla Firefox)
- Probleme mit lokal angeschlossener Peripherie (Maus, Tastatur, Monitor, Drucker etc.)
- Probleme mit der Netzwerk-Infrastruktur (Switch, Router, Firewall etc.)

Auch bei Problemen mit IT-Zulieferern wie z.B. Internet Providern helfen wir weiter, sofern dies gewünscht ist. Dazu zählt insbesondere:

- Meldung von Problemen bei Ihrem Vertragspartner
- Begleitung der Problemlösung durch den Vertragspartner

- Kommunikation von Statusinformationen von Ihnen bzw. des Vertragspartners

Die Lösung der Probleme obliegt hierbei dem IT-Zulieferer selbst.

2.10 Umfassende Administrationstätigkeiten

- Bereitstellung von Informationen über die aktuell vorliegende Konfiguration
- Zurücksetzen eines Passwortes (bspw. nach Ablauf, bei Verlust)
- Eingliederung neuer Mitarbeiter
- Änderung von Benutzereinstellungen (Name, Standort etc.) und Berechtigungen
- Ausgliederung ehemaliger Mitarbeiter
- Anlage und Pflege einer IT-Dokumentation
- Einrichtung und Inbetriebnahme von Arbeitsplätzen als Maßnahmen im Rahmen einer konkreten Störungsbehebung (inkl. Auslieferung, sofern der IT. Läuft. Premium Service gebucht wurde)
- Mitnahme und Entsorgung alter Arbeitsplätze (ggf. zzgl. Aufschlag für BSI-konforme Löschung)
- Änderungen in Ihrem Verzeichnis, insbesondere
    - Definition der Zugriffsrechte im Netzwerk sowie auf die Anwendungen
    - Benutzerverwaltung
    - Hardwareverwaltung
- administrative Anpassungen (Pflege, Wartung und kleine Änderungen) an der Konfiguration der Netzwerk-Infrastruktur (Switch, Router, Firewall etc.), insbesondere im Rahmen einer konkreten Störungsbehebung
- Pflege und Anpassung der notwendigen DNS-Einträge Ihrer individuellen Domain (Voraussetzung: Bereitstellung administrativer Zugangsdaten auf die vorhandene Domain)
- Installation von Office-Programmen auf Ihren Geräten im Rahmen einer konkreten Störungsbehebung
- Bearbeitung von Störungen an oder das Einspielen von Software-Updates bei Anwendungsprogrammen oder Branchenlösungen in der jeweils vom Hersteller angebotenen, aktuellsten Version, sofern gemeinsam schriftlich vereinbart. Eine Liste der im individuellen Leistungsumfang enthaltenen Programme pflegen wir in unserer Kundendokumentation und stellen Ihnen diese auf Anfrage gerne zur Verfügung

2.11 Koordination externer Dienstleister

- Änderungen an der Verkabelung von Netzwerk und Elektrik
- Probleme, Störungen und Anpassungswünsche im Bereich Telefonie / VoIP

2.12 Unsere Servicezeiten

Wir sind von Montag bis Freitag von 7.00 Uhr bis 18.00 Uhr für Sie erreichbar. Eine Störungsannahme erfolgt darüber hinaus Montag bis Freitag von 18.00 Uhr bis 20.00 Uhr sowie am Samstag von 09.00 Uhr bis 13.00 Uhr. Ausgenommen sind bundesweit geltende Feiertage. Sollten Sie Bedarf für darüber hinausgehende Erreichbarkeiten haben, sprechen Sie uns an. Meist finden wir auch dafür eine Lösung.

Sollten Arbeiten außerhalb der Servicezeiten notwendig sein, werden diese mit einem Aufschlag abgerechnet. Eine entsprechende Aufstellung stellen wir Ihnen gerne zur Verfügung.

2.13 Nicht enthaltene Leistungen

Alle in den vorhergegangenen Abschnitten beschriebenen Leistungen und Services der IT. Läuft. Pakete beziehen sich nur auf von uns vertriebene bzw. unterstützte Hardware und Services. Sollten Sie darüber hinaus Unterstützung bei der laufenden Betreuung einer Lösung oder eines Produktes benötigen, helfen wir Ihnen gerne bei der Suche nach einem passenden Dienstleister. Uns im Rahmen des Supports dieser Lösungen oder Produkte entstehenden Kosten Dritter, die gesondert in Rechnung gestellt werden. Selbstverständlich werden wir jedoch im Einzelfall darauf hinweisen, sobald dieser Fall eintritt.

Vor-Ort Einsätze

Vor-Ort-Einsätze sind im IT. Läuft. sowie im IT. Läuft. Plus Paket nicht enthalten und werden gesondert abgerechnet. Um eine noch bessere Planbarkeit Ihrer IT-Kosten zu bekommen, empfehlen wir das IT. Läuft. Premium Paket.

Beseitigung von vermeidbaren Störungen und Schäden

Damit meinen wir Beschädigungen, die durch nicht angemessene Behandlung oder absichtliche Einwirkung von Ihnen oder Außenstehenden verursacht werden. Dazu gehört auch die Löschung von Dateien oder Verzeichnissen oder Software-Installationen. Die Beseitigung von Störungen und Schäden, die durch Umweltbedingungen am Aufstellungsort oder durch Fehler in der Stromversorgung verursacht werden, die Bekämpfung von Schadsoftware jeglicher Art auf Server- und Arbeitsplatz-Systemen sowie die Bereitstellung von Ersatzteilen, Verbrauchsmaterialien und Kleinteilen (beispielsweise Kabel, Befestigungsmaterialien, Toner, Tinte, etc.) für Hardware sind ebenfalls nicht im Leistungsumfang enthalten.

Größere Veränderungen an den Systemen

Hierzu zählen beispielsweise die Neu-Installation von Servern, das Austauschen von Firewalls, das Etablieren standortübergreifender VPN-Verbindungen, Verkabelungsarbeiten, die Migration von Exchange-Servern zu Microsoft 365 oder die Integration und Konfiguration von Telefonanlagen in die vorhandene Infrastruktur. Auch ein Austausch von Arbeitsplätzen und der Versionswechsel des Betriebssystems eines Arbeitsplatzes oder Servers ist nicht enthalten. Arbeiten, die nicht unter den Leistungsumfang fallen, werden im Vorfeld mit Ihnen besprochen und nach Beauftragung, basierend auf einem gesonderten Angebot, abgerechnet.

Änderungsanforderungen

Von Ihnen gewünschte Änderungsanforderungen von üblichen Einstellungen sind grundsätzlich enthalten. Für die Umsetzung und ggf. benötigte Lizenzen und Hardware erhalten Sie ein gesondertes Angebot. Dazu zählen insbesondere:

- Verlängerung von Hersteller-Support- / Wartungsverträgen
- Verlängerung von Lizenzen für Datensicherungssoftware uvm.
- physischer Umzug eines einzelnen Arbeitsplatzes an einen anderen Standort

Behebung von Störungen an Anwendungsprogrammen oder Branchenlösungen

Die Behebung von Störungen an speziellen Anwendungsprogrammen oder Branchenlösungen ist nicht enthalten, sofern wir nichts anderes gemeinsam vereinbart haben. Insbesondere betrifft dies folgende Software:

- Warenwirtschafts- oder ERP-Systeme wie SAP, Sage, Lexware uvm.
- Buchhaltungsprogramme wie DATEV, Lexware uvm.
- CAD-Software wie AutoCAD uvm.
- DMS-Systeme wie ELO, Develop, EcoDMS uvm.

3. IT. Läuft. Plus Paket

Die Leistungen im IT. Läuft. Plus Paket gehen über die Leistungen des IT. Läuft. Pakets hinaus und erweitern diese insbesondere um zusätzliche Leistungen im Bereich IT-Sicherheit.

3.1 Active Directory und Entra ID Sicherheitsmanagement

Die zentrale Verwaltung von Benutzer- und Computerzugängen sowie Sicherheitsrichtlinien - insbesondere über Microsoft Active Directory und Entra ID - ist ein Hauptziel für Cyberangriffe. Über 90 % aller erfolgreichen Angriffe nutzen Schwachstellen in diesen Systemen. Unsere Lösung schützt die Identitätsdienste proaktiv und nachhaltig vor Bedrohungen und sorgt für eine kontinuierlich sichere Umgebung.

Aufgrund der dynamischen Bedrohungslage und sich wandelnder Anforderungen ist eine fortlaufende Überwachung und Anpassung unerlässlich. Ein einmaliges Setup reicht nicht aus.

Enthaltene Leistungen

Echtzeit-Monitoring – Bedrohungen erkennen

Wir überwachen Ihre Active Directory- und Entra ID-Umgebung kontinuierlich. Sicherheitsrelevante Ereignisse werden in Echtzeit erkannt und gemeldet, sodass eine schnelle Reaktion möglich ist.

Automatisierte Schwachstellenanalyse – Risiken frühzeitig identifizieren

Unsere Plattform scannt regelmäßig Ihre Identitätsinfrastruktur auf Fehlkonfigurationen und potenzielle Schwachstellen. Diese werden priorisiert und klassifiziert, um gezielte Maßnahmen zu ermöglichen.

Angriffserkennung – Schutz vor gezielten Attacken

Durch fortschrittliche Analysemethoden erkennen wir gezielte Angriffe frühzeitig und helfen, diese abzuwehren, bevor Schaden entsteht.

Forensische Analyse – revisionssicher dokumentiert

Wir halten automatisch fest, wer was wann getan hat und das revisionssicher. Hilfreich für schnelle Ursachenklärung und für Compliance-Nachweise.

Nicht enthaltene Leistungen

Behebung von Angriffsschäden

Die Leistung umfasst nicht die Wiederherstellung nach einem erfolgreichen Angriff. Selbstverständlich stehen wir Ihnen auch in solchen Fällen zur Seite – diese Leistungen werden separat abgerechnet.

3.2 Digitale Lernplattform inklusive IT-Sicherheitsschulungen

Der Schlussel zu einer erhöhten IT-Sicherheit liegt in der Schulung und Sensibilisierung der Menschen im Unternehmen. Die meisten Datenverluste durch Cyberangriffe ließen sich vermeiden, wenn Mitarbeitende besser informiert und aufgeklart waren. Selbst die beste Technik ist wirkungslos, wenn die Anwendenden die IT-Sicherheitsrisiken nicht kennen. Neben den notigen technischen Losungen bieten wir daher fortlaufende IT-Sicherheitstrainings an.

Im Rahmen der Cyber-Versicherung, DSGVO, NIS2 und diverser ISO-Zertifizierungen sind Unternehmen verpflichtet, ihre Mitarbeitenden fur das Thema IT-Sicherheit fortlaufend zu sensibilisieren.

Enthaltene Leistungen

Simulierte Phishing-Angriffe

Wie reagieren die Mitarbeitenden auf Phishing-E-Mails? Anhand der Auswertung realitätsgetreu imitierter Phishing-E-Mails erhalten Sie zweimal jährlich eine fundierte Aussage über den Umgang mit täglich vorkommenden Cyber-Angriffen in Ihren Unternehmen.

E-Learning Plattform

Nachdem die Ergebnisse der initialen Phishing-Kampagne vorliegen, wird die TÜV-zertifizierte Schulungsplattform von uns freigeschaltet. Enthalten sind verschiedene kurze Trainings zu IT-Sicherheitsthemen, die nach und nach freigegeben werden. Ausgewählte Nutzer erhalten Einblick in die Teilnahmestatistik der Mitarbeiter. Für erfolgreich abgeschlossene Trainings werden den Mitarbeitern personenbezogene, rechtskraftige Zertifikate bereitgestellt.

Optionale Leistung

IT-Sicherheitsschulung

Diese optional buchbare Schulung beinhaltet eine Vor-Ort-Schulung durch uns, um zwischen Versand der Phishing-E-Mail und der E-Learning-Phase für das Thema IT-Sicherheit zu sensibilisieren. Die Ergebnisse der Versandphase können genutzt werden, um den Mitarbeitern ganz konkret die Problematik aufzuzeigen. In erster Linie ist diese Schulung jedoch eine unterhaltsame Veranstaltung mit nachhaltigem AHA-Effekt und viel Inhalt aus der Praxis.

3.3 IT-Sicherheitsberatung für Geschäftsleitungen

Die IT-Sicherheitsexperten von einsnulleins führen halbjährlich Gespräche mit Ihrer Geschäftsleitung, in denen sie umfassend über aktuelle Themen der IT-Sicherheit sowie erforderliche Maßnahmen informieren. Dabei berücksichtigen wir die geltenden gesetzlichen Vorgaben, analysieren detailliert den Status der IT-Sicherheit im Unternehmen und untermauern diese Analyse durch KPI-Werte sowie durch konkrete Handlungs- und Maßnahmenpläne.

4. IT. Läuft. Premium Paket

Die Leistungen im IT. Läuft. Premium Paket werden gegenüber den Leistungen des IT. Läuft. Plus Paketes um den Vor-Ort-Service erweitert.

Im Rahmen dieses Pakets übernehmen wir außerdem die Rolle eines externen IT-Leiters für Sie. Die Security-Beratungen erfolgen vierteljährlich. Zudem beraten wir die Geschäftsleitung fortlaufend bei der Weiterentwicklung der IT-Security und IT-Infrastruktur und begleiten sie auf Wunsch auch in strategischen Fragen zur Unternehmensentwicklung Darüber hinaus sind wir Ihr erster Ansprechpartner in folgenden Punkten:

- zentraler Ansprechpartner für alle IT-Anliegen und Probleme
- Beratung und Unterstützung bei Digitalisierungsprojekten
- Durchführung von Schulungen einzelner Mitarbeiter im Bereich Standardsoftware
- Kommunikation und Koordination der Hardware-Lieferanten
- Kommunikation und Koordination aller Angelegenheiten mit den vorhandenen und zukünftigen Softwarelieferanten

Damit haben Sie die größtmögliche Kostensicherheit für den laufenden Betrieb der bestehenden Infrastruktur.