TECHNISCHE DATEN

Stand: 12.2017 / Version: 1.1

SICHERHEIT

Wir schaffen Lösungen für die konkreten Bedrohungen Ihrer Systeme und Daten. Den Vorgaben und Empfehlungen des BSI folgen wir dabei genauso wie internationale ‚Best Practice' Beispielen und tagesaktuellen Entwicklungen.

- Segmentierung des Netzwerks entsprechend der Verletzlichkeit/Angreifbarkeit
- Filter und Zugriffssteuerung auf Netzwerkebene (Whitelisting)
- Überwachung des Netzwerkverkehrs auf ungewöhnliche Muster und Zugriffsversuche
- Schnelle Isolierung erfolgreich angegriffener Systeme
- Viren Scans für alle ankommenden und zu sendenden Emails

DATENSCHUTZ

Mit der Verschärfung des BDSG[1] in 2008, den Urteilen des EUGH aus 2016 und der Einführung der DSGVO[2] hat der Datenschutz einen neuen Stellenwert erhalten. Der Geschäftsführer ist jetzt persönlich haftend, was bei personenbezogen Daten im Strafrecht und Firmengeheimnissen im Zivilrecht gravierende Konsequenzen haben kann.

- Dokumentation aller relevanten Netzwerk-Komponenten
- Sicherung vor physischem Zugriff durch unberechtigte Dritte
- Schutz aller Netzwerk-Komponenten durch starke Passwörter und Zugriffsschutz
- Starke Verschlüsselung von Datenübertragungen über unsichere Verbindungen
- Schulung der Mitarbeiter

VERFÜGBARKEIT

Durch sinnvolle Redundanzen und ausreichend dimensionierte Überbrückungssysteme sichern wir den Betrieb bei den häufigsten Störungen. Zusätzlich sorgen automatisierte Prozesse und Abläufe für eine sichere Abschaltung und Wiederanlauf Ihrer Systeme bei schweren Ausfällen.

- Priorisierung von Telefonie und Dialoganwendungen (Warenwirtschaft etc.) in allen Netzwerksegmenten
- Zwei Außenanbindungen mit unterschiedlicher Technik (DSL/Kabel/Glasfaser) bei verschiedenen Anbietern im automatischen ‚Fail-Over'
- Unterbrechungsfreie Stromversorgung für alle Netzwerkkomponenten mit einer Pufferzeit von 30 Minuten einschließlich Notrufsystemen und Telefonen
- Störungsmeldung und -verfolgung bei Internetanbietern, Stromversorgern und Dienstleistern
- Automatische kontrollierte Abschaltung (Herunterfahren) bei länger andauernden Ausfällen um Datenverlust und Beschädigungen zu vermeiden

WARTUNG UND SERVICE

Vorbeugende jährliche Wartung und Prüfung der elektrischen Betriebssicherheit sowie kostenloser Tausch von Komponenten bei ersten Anzeichen einer Alterung helfen die Ursachen für Ausfälle zu reduzieren.

- Prüfung der elektrischen Betriebssicherheit aller Netzwerkkomponenten nach VDE-0100-600[3]
- SMART[4] Monitoring und Tausch von Festplatten
- Reinigung aller Kühler und Lüfter zur Vermeidung von Überhitzung
- Test der unterbrechungsfreien Stromversorgung und Austausch von gealterten Batterien

UMSTELLUNG

Mit der Übernahme des Netzwerkmanagements und dem Austausch der Komponenten und der Einführung aller beschriebenen Funktionen erfolgt die Integration in unsere Betriebsübewachung und Betrieb. Dies erfolgt außerhalb der Geschäftszeiten nach Vereinbarung.

- Detaillierte Bestandsaufnahme des Netzwerks und aller angeschlossenen Geräte
- Planung der neuen Netzwerkstruktur, Adressierung und Komponenten entsprechend der Vorgaben aus Datenschutz und Sicherheit auf Basis unserer geprüften Vorlagen
- Abstimmung der Zeitplanung für die Umstellung mit Ihnen und betroffenen Dritten (Internet Provider für DNS und Email)
- Gemeinsame Abnahme nach Abschluss der Umstellung und Übergabe der vollständigen Dokumentation in schriftlicher und elektronischer Form

NETZWERK

Für uns ist das Netzwerk die zentrale Komponente und die Basis Ihrer gesamten IT, Überwachungs- und Telefoninfrastruktur. Zukunftssicher und sinnvoll dimensioniert erfüllt es nicht nur aktuelle Anforderungen sondern schafft vor allem die Flexibilität zur schnellen und kostengünstigen Umsetzung neuer Technologien und Anwendungen.

- Konfiguration und Betrieb der von uns kostenlos zur Verfügung gestellten Switche und Firewall
- Eindeutige farbliche Kennzeichnung aller Ports und Erneuerung der Patch Verkabelung[5] mit entsprechenden Kabeln
- Permanente Überwachung des Datenvolumen aller Netzwerkanschlüsse und Segmente sowie aller aktiven Netzwerkkomponenten
- Zeitnahe Aktualisierung der Firmware aller Systeme ab Freigabe durch den Hersteller

[1] Vorhandene Kabel werden so weit wie möglich weiter verwendet
[2] Datenschutzgrundverordnung
[3] Regelmäßige Prüfung elektrischer Anlagen nach dem Errichten, dem Erweitern oder dem Ändern solcher Anlagen
[4] Self-Monitoring, Analysis and Reporting Technology dient der Vorhersage eines möglichen Ausfalls des Speichermediums
[5] Vorhandene Kabel werden so weit wie möglich weiter verwendet
[6] Verbindungen aus dem WLAN/Hotspot werden über die zentrale Firewall gesteuert und kontrolliert
[7] EC-Karten Terminals, ExtraNet, EDI
[8] Bei sehr großen Postfächern (mehr als 5GByte) kann es zu Verzögerungen beim Start der eMail-Anwendung kommen
[9] Optional beim Einsatz von Emails als Geschäftsbrief
[10] Microsoft Windows, Apple OSX, Apple IOS, Google Android

WLAN

Ob mobile Endgeräte Ihrer Mitarbeiter oder ein kostenloser Internet-Zugang für Ihre Kunden, ein sicheres und leistungsfähiges WLAN ist in vielen Betrieben heute unverzichtbar. Rechtssicherheit beim Betrieb von Hotspots sowie die Sicherheit Ihrer Daten sind dabei die Grundvoraussetzung und werden von uns garantiert.

- Ausmessen / Ausleuchten Ihrer Geschäftsräume zur Planung und Dimensionierung des Netzwerks
- Installation und Konfiguration aller Zugangspunkte / Basisstationen
- Betrieb erfolgt in einem eigenen Netzwerksegment ohne direkte Verbindung[6] zu anderen Netzwerksegmenten
- Authentifizierung für eigene Geräte und die Geräte von Mitarbeitern sowie Verschlüsselung aller Übertragungen
- Konfiguration einer Informationsseite für Hotspot Nutzer (Captive Portal) mit allen rechtlichen Angaben

INTERNET

Da inzwischen auch Telefonie und viele Anbindungen mit Partnern über das Internet abgewickelt werden ist ein funktionsfähiger Zugang kritisch für den täglichen Betrieb. Redundante Anschlüsse, die auf unterschiedlichen Technologien aufbauen und von verschiedenen Anbietern betrieben werden, helfen bei Ausfällen eines Anschlusses sicher weiter arbeiten zu können und ermöglichen den Einsatz robuster kostengünstiger Standardprodukte.

- Installation und Konfiguration der Modems für DLS, Kabel und Glasfaser
- Einrichten eines automatischen Fail-Overs bei Ausfall einer Verbindung
- Konfiguration von speziellen Firewall-Filterregeln für Zugriffe auf Partnersysteme[7]
- Permanente Überwachung der Außenanbindungen und automatische Meldung von Störungen
- Management von Störungen und deren Behebung in Ihrem Namen

EMAIL

Neben Telefonie ist Email das zweite unverzichtbare Kommunikationsmittel im täglichen Gebrauch. Ob Anfragen von Kunden oder Abstimmungen mit Lieferanten, ohne einen zuverlässigen und vor allem sicheren Betrieb der Email ist ein professionelles Arbeiten nicht mehr denkbar. Wir bieten eine auf die Anforderungen im Handel zugeschnittene Plattform, ohne dass Sie eigene Systeme betreiben müssen.

- Bis zu 4 Email-Konten (IMAP-Konten) pro Mitarbeiter
- Beliebig viele Email-Adressen pro Mitarbeiter
- Keine Begrenzung des Speicherplatzes[8] pro Email-Konto
- Import Ihrer vorhandenen Emails auf unser System
- Alle verschickten und empfangenen Emails werden auf Viren und SPAM untersucht
- Der Betrieb eines Backup Email Servers (Secondary MX) an einem zweiten Standort verhindert den Verlust von Emails bei Störungen
- Automatische Abwesenheitsnotiz bei Urlaub
- Spezielle abgesicherte Email-Konten für Systeme zum Datenaustausch
- Optional Archivierung[9] von Emails unter Einhaltung der Vorschriften nach GOBD

REMOTE ACCESS

Der Zugriff auf Email, Kalender, Kontakte und Systeme von Unterwegs oder aus dem Home Office ist inzwischen Standard. Sichere und zuverlässige Zugängen für alle Mitarbeiter sind natürlich Teil des Angebots.

- Stark verschlüsselte Verbindungen nach dem IPsec Standard
- Keine Zusatzsoftware durch den Einsatz der Microsoft / Apple / Google[10] Systemprogramme
- Automatische Updates und Sicherheits-Patches durch Microsoft / Apple / Google
- Passwort oder Zertifikatsbasierte Authentifizierung

STANDORT VERNETZUNG

Außenstellen, Lager oder Filialen werden kostengünstig an die Zentrale angebunden oder untereinander vernetzt.

- Stark verschlüsselte Verbindungen nach dem OpenVPN Standard
- Transparenter Zugriff auf alle Ressourcen der Zentrale und umgekehrt
- Telefonie, Daten und Überwachung
- Einsatz kostengünstiger und ausfallsicherer Standardprodukte im Fail-Over wie beim Hauptzugang
- Internet Zugang über zentrale Firewall gesichert

ÜBERWACHUNG

Störungen und Probleme erkennen wir im Idealfall noch bevor sie den Betrieb beeinflussen durch unsere Systemüberwachung und Alarmierung.

- 24/7 Überwachung aller aktiven Netzwerkkomponenten, Anbindungen, Komponenten, Verbindungen und Stromversorgung
- Alarmierung und Benachrichtigung eines Ansprechpartners in Ihrem Haus
- Automatische Störungsmeldung bei Internet- und Telefon- Anbietern
- Störungsmanagement mit Anbietern in Ihrem Namen

STROMVERSORGUNG

Neben echten Unterbrechungen der Stromversorgung bereiten besonders Spannungs- und Frequenz-Schwankungen, sogenannte Brown-Outs, immer wieder Probleme. Daher werden alle Systeme aus Gründen der Stabilität und Verfügbarkeit nur über eine zwischengeschaltete Unterbrechungsfreie Stromversorgung betrieben.

- Alle aktiven Netzwerkkomponenten, Modems und Netzabschluss-Komponenten für 30 Minuten batteriegepuffert
- Automatische kontrollierte Abschaltung aller aktiven Netzwerkkomponenten nach 30 Minuten um Datenverlust zu vermeiden
- Selbständiger Wiederanlauf aller Netzwerkkomponenten nach Wiederherstellung der Stromversorgung