buschkamp
Kompetent fürs Büro

APELT - GRUPPE

IT-SERVICE

SICHERHEITSLÜCKEN ERKENNEN.

RISIKEN MINIMIEREN - IT SCHÜTZEN.

DIE WICHTIGSTEN IT-SICHERHEITSTHEMEN IM ÜBERBLICK:

Plus:

INKL. PRAXIS-CHECKLISTE



Habbesweg 1
59427 Unna

Telefon: 02303 - 25 14 00
Email: info@buschkamp.de

www.buschkamp.de

buschkamp
Kompetent fürs Büro

IT-SERVICE

Ihr Partner für zukunftssichere IT-Systeme und IT-Sicherheit

Über 80 Jahre Expertise für Ihren Geschäftserfolg: Als Mitglied der etablierten **Apelt-Gruppe** vereint Buschkamp fundierte Branchenerfahrung mit moderner technologischer Expertise.
Wir begleiten kleine Unternehmen sowie den gehobenen Mittelstand bei der zukunftssicheren Digitalisierung, Systemintegration und ganzheitlichen Absicherung ihrer IT-Infrastruktur.

1. IT-Sicherheit & Proaktiver Schutz

In einer vernetzten Geschäftswelt ist eine lückenlose Cybersicherheit das Fundament ungestörter Betriebsabläufe. Buschkamp schützt vertrauliche Unternehmensdaten und verhindert Ausfallzeiten durch mehrstufige Sicherheitskonzepte:

- ***Mehrstufige Cybersicherheit:*** Schutz vor Bedrohungen durch hochmoderne Firewalls, Antivirus-Software und Verschlüsselungstechnologien.
- ***Proaktive Überwachung & Wartung:*** Kontinuierliches System-Monitoring erkennt Risiken frühzeitig und behebt Störungen, bevor Ausfälle entstehen.
- ***DSGVO-konforme Datensicherheit:*** Physischer Datenschutz durch Hochleistungs-Aktenvernichter gemäß DSGVO und ISO 21964.

2. IT-Infrastruktur & Skalierbare Hardware

Auf Basis detaillierter Hardware-Bedarfsanalysen schaffen wir eine leistungsstarke und erweiterbare IT-Landschaft, die exakt auf Ihre geschäftlichen Anforderungen abgestimmt ist:

Bereich	Komponenten & Lösungen	Kundennutzen
Server & Speichersysteme	High-End Server, NAS-Systeme, Cloud-Speicher (SaaS / IaaS)	Hohe Datenverfügbarkeit & flexible Skalierbarkeit
Netzwerkinfrastruktur	Moderne Router, Switches, Access Points & WLAN-Lösungen	Stabile, sichere & schnelle Datenübertragung
Arbeitsplatz-Hardware	Desktops, Laptops, Workstations & Ergonomie-Zubehör	Optimal ausgestattete & produktive Mitarbeiter

3. Intelligentes Dokumentenmanagement (DMS) & Mobiles Arbeiten

Ein modernes Dokumentenmanagement-System (DMS) strukturiert Ihre Workflows und sorgt für die sichere, zentrale Ablage aller geschäftskritischen Dokumente. Rollenbasierte Zugriffsrechte und automatisierte Prozesse garantieren maximale Effizienz – auch beim mobilen Arbeiten im Homeoffice oder unterwegs.

4. IT-Entlastung mit voller Planungssicherheit

Ressourcen freisetzen:
Durch die Auslagerung zeitintensiver IT-Aufgaben an das erfahrene Support-Team von Buschkamp konzentrieren Sie sich voll auf Ihr Kerngeschäft. Zum monatlich attraktiven Festpreis profitieren Sie von reibungslos funktionierenden Systemen, schnellem Service und absoluter Transparenz.

Ihr Vorteil:
Ganzheitlicher Service & IT-Betreuung aus einer Hand.

Cyberangriffe – IT-Sicherheit bleibt eine zentrale Herausforderung

Die digitale Vernetzung bietet Unternehmen zahlreiche Möglichkeiten, bringt jedoch auch wachsende Sicherheitsrisiken mit sich. Cyberkriminelle entwickeln ihre Methoden kontinuierlich weiter und nehmen dabei Unternehmen jeder Größe ins Visier. Wie ernst die Situation inzwischen ist, zeigt auch die jährliche Analyse des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Einschätzung der Behörde fällt deutlich aus:
Die Bedrohungslage im Bereich der IT-Sicherheit bleibt angespannt und besorgniserregend.

Vielfältige Angriffsmethoden setzen Unternehmen unter Druck

Die Gefahren gehen von unterschiedlichen Tätergruppen und Angriffsszenarien aus.
Dazu gehören Wirtschaftsspionage, der gezielte Diebstahl vertraulicher Zugangsdaten sowie Angriffe über Sicherheitslücken, die noch nicht durch Updates geschlossen wurden.
Auch professionell organisierte Cybercrime-Gruppen nutzen immer ausgefeiltere Techniken, um in Unternehmensnetzwerke einzudringen.

Die wirtschaftlichen Folgen sind erheblich: Datenverluste, Produktionsausfälle, Betriebsunterbrechungen und Industriespionage verursachen in deutschen Unternehmen Schäden in Milliardenhöhe. Besonders kritisch sind Angriffe, bei denen sensible Informationen entwendet oder ganze IT-Systeme lahmgelegt werden.

Auch gezielte Angriffe auf deutsche Unternehmen nehmen zu

Cyberattacken sind längst keine abstrakte Gefahr mehr. Immer wieder geraten deutsche Unternehmen, öffentliche Einrichtungen und Organisationen ins Visier internationaler Hackergruppen. Betroffen sind unter anderem Betriebe aus den Bereichen Logistik, Rüstung, IT-Dienstleistungen sowie Luft- und Raumfahrt. Aber auch Verbände und Stiftungen bleiben nicht verschont.

Die Hintergründe solcher Angriffe sind unterschiedlich: Während manche Tätergruppen finanzielle Interessen verfolgen, geht es anderen um Spionage, Sabotage oder die Beschaffung vertraulicher Informationen.

Ransomware und DDoS gehören zu den größten Risiken

Die Bandbreite digitaler Bedrohungen ist groß. Besonders auffällig sind umfangreiche DDoS-Attacken, bei denen Server und Online-Dienste durch eine enorme Anzahl gleichzeitiger Anfragen überlastet werden. Auch Cloud-Systeme und digitale Infrastrukturen geraten zunehmend ins Visier von Angreifern.

Eine weitere erhebliche Gefahr stellen sogenannte Ransomware-Angriffe dar. Dabei verschlüsseln Kriminelle Unternehmensdaten und fordern anschließend Lösegeld für deren Freigabe. Besonders kleine und mittelständische Unternehmen sind gefährdet, wenn Sicherheitsmaßnahmen nicht ausreichend umgesetzt wurden.

Wie schwerwiegend die Auswirkungen sein können, zeigen auch Angriffe auf kommunale IT-Dienstleister: Bereits einzelne Vorfälle können zahlreiche angeschlossene Städte und Gemeinden gleichzeitig betreffen und deren Arbeitsabläufe erheblich beeinträchtigen.

Unser Tipp von Buschkamp:
Warten Sie nicht, bis ein Sicherheitsvorfall eintritt. Eine gut geschützte IT-Infrastruktur, regelmäßige Sicherheitsupdates, zuverlässige Datensicherungen und ein durchdachtes Sicherheitskonzept helfen dabei, Risiken frühzeitig zu reduzieren.

Wir helfen Ihnen dabei!

buschkamp
Kompetent fürs Büro

IT-SERVICE

Cyberkriminalität kennt keine Grenzen – jedes Unternehmen kann betroffen sein

Cyberangriffe richten sich längst nicht mehr ausschließlich gegen große Konzerne. Auch kleine und mittelständische Betriebe sowie öffentliche Einrichtungen geraten zunehmend ins Visier von Cyberkriminellen. Gerade Unternehmen mit kritischen Infrastrukturen (KRITIS) müssen dabei besondere gesetzliche Sicherheitsanforderungen erfüllen.

DIESE BEREICHE SIND BESONDERS IM FOKUS:

GESUNDHEITSWESEN

Arztpraxen, Krankenhäuser und Pflegeeinrichtungen arbeiten täglich mit hochsensiblen persönlichen Daten. Gelangen diese in falsche Hände, kann das schwerwiegende Folgen haben. Entsprechend attraktiv sind solche Einrichtungen für Erpressungsversuche und Datendiebstahl.



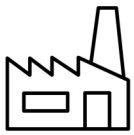
BANKEN UND FINANZDIENSTLEISTER

Finanzunternehmen verfügen über wertvolle Kunden- und Kontoinformationen. Angreifer versuchen, sich Zugang zu Zahlungsdaten, Bankkonten und internen Finanzsystemen zu verschaffen, um daraus finanziellen Nutzen zu ziehen.



INDUSTRIE UND PRODUKTION

Moderne Fertigungsbetriebe sind auf miteinander vernetzte Maschinen, Anlagen und IT-Systeme angewiesen. Wird diese Infrastruktur angegriffen, können Produktionsabläufe stillstehen und erhebliche wirtschaftliche Schäden entstehen.



BEHÖRDEN UND ÖFFENTLICHE EINRICHTUNGEN

Kommunale Verwaltungen und öffentliche Institutionen speichern große Mengen vertraulicher Bürgerdaten. Ein erfolgreicher Cyberangriff kann nicht nur den Datenschutz gefährden, sondern auch wichtige Verwaltungsleistungen und öffentliche Dienstleistungen beeinträchtigen.



ABER ES GIBT GUTE NACHRICHTEN!

Unternehmen sind Cyberangriffen nicht schutzlos ausgeliefert. Wer mögliche Gefahren kennt, Sicherheitslücken rechtzeitig erkennt und geeignete Schutzmaßnahmen einsetzt, kann das Risiko deutlich reduzieren. Entscheidend sind eine gut abgesicherte IT-Infrastruktur, regelmäßige Kontrollen und ein klarer Notfallplan.

Buschkamp unterstützt Sie dabei, Ihre IT sicherer zu machen –
damit Sie sich auf Ihr Kerngeschäft konzentrieren können.

IT-SERVICE

buschkamp
Kompetent fürs Büro

Hacker schlafen nicht – schützen Sie Ihre IT, bevor es zu spät ist!

Die zunehmende Digitalisierung macht viele Unternehmensabläufe schneller und effizienter. Gleichzeitig wachsen jedoch auch die Anforderungen an den Schutz Ihrer IT-Systeme. Cyberkriminelle nutzen gezielt veraltete Software, ungeschützte Geräte und bekannte Sicherheitslücken, um sich Zugang zu Unternehmensnetzwerken zu verschaffen.

Eine wichtige Grundregel lautet deshalb: Halten Sie Ihre Hard- und Software konsequent auf dem neuesten Stand. Regelmäßige Updates für Betriebssysteme, Anwendungen und Geräte-Firmware schließen bekannte Schwachstellen und erschweren Angreifern den Zugriff.
Moderne Sicherheitslösungen können zusätzlich verdächtige Aktivitäten erkennen und bei ungewöhnlichen Vorgängen automatisch Alarm schlagen.

Dabei sollte nicht nur ein einzelner Computer betrachtet werden. Entscheidend ist, dass sämtliche Geräte und Systeme innerhalb Ihres Unternehmens zuverlässig abgesichert sind – vom Arbeitsplatz-PC über mobile Endgeräte bis hin zu Druckern und Netzwerkkomponenten.

SICHERHEIT IST KEIN EINMALIGES PROJEKT

Die Methoden von Cyberkriminellen verändern sich ständig. Was heute noch als sicher gilt, kann bereits morgen neue Risiken aufweisen. Deshalb reicht es nicht aus, einmalig Schutzmaßnahmen einzurichten und sich anschließend darauf zu verlassen.

Ein nachhaltiges Sicherheitskonzept benötigt regelmäßige Überprüfungen, klare Zuständigkeiten und eine kontinuierliche Anpassung an neue Bedrohungen. Orientierung bietet unter anderem der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI).
Im Mittelpunkt stehen dabei drei wesentliche Schutzziele:

- **Vertraulichkeit:** Informationen dürfen nur von berechtigten Personen eingesehen werden.
- **Integrität:** Daten müssen vollständig und unverändert bleiben.
- **Verfügbarkeit:** Systeme und Informationen müssen bei Bedarf zuverlässig erreichbar sein.

BUSCHKAMP – IHR PARTNER FÜR EINE SICHERE IT

Ob moderne Hardware, aktuelle Software oder ganzheitliche IT-Sicherheitslösungen: Buschkamp unterstützt Unternehmen dabei, ihre technische Infrastruktur zuverlässig und zukunftssicher aufzustellen. Dazu gehören der Schutz Ihrer IT-Systeme, sichere Druck- und Netzwerklösungen sowie die Überwachung wichtiger Komponenten.

Unser Anspruch: Technik, Sicherheit und Service sinnvoll miteinander verbinden – abgestimmt auf die Anforderungen Ihres Unternehmens.





buschkamp
Kompetent fürs Büro

IT-SERVICE

Neue Anforderungen an die IT-Sicherheit: NIS-2

Drucker und Multifunktionsgeräte sind längst ein fester Bestandteil moderner Unternehmensnetzwerke. Sie verarbeiten vertrauliche Daten, kommunizieren mit anderen Systemen und können bei unzureichendem Schutz zum Einfallstor für Cyberangriffe werden.

Deshalb müssen auch Drucksysteme konsequent abgesichert werden. Veraltete Software, fehlende Updates oder ungeschützte Zugänge erhöhen das Sicherheitsrisiko erheblich.

Zusätzliche Bedeutung erhält dieses Thema durch die NIS-2-Richtlinie. Sie verschärft die europäischen Anforderungen an die Cybersicherheit und verpflichtet betroffene Unternehmen zu umfangreicheren Schutzmaßnahmen.

DIE WICHTIGSTEN ANFORDERUNGEN IM ÜBERBLICK:

- **Risikomanagement:** Gefahren erkennen, bewerten und gezielt reduzieren.
- **Notfallmanagement:** Klare Abläufe für die schnelle Reaktion auf Cyberangriffe festlegen.
- **Zugriffsschutz:** Benutzerkonten und Zugriffsrechte zuverlässig absichern.
- **Dienstleister:** Auch externe Partner auf ihre Sicherheitsstandards überprüfen.
- **Meldepflichten:** Bestimmte Sicherheitsvorfälle innerhalb von 24 Stunden melden.
- **Berichterstattung:** Innerhalb von 72 Stunden einen ausführlicheren Bericht vorlegen.
- **Kontrollen:** Sicherheitsmaßnahmen regelmäßig überprüfen und anpassen.



Wichtig:

NIS-2 gilt nicht automatisch für jedes Unternehmen. Entscheidend sind unter anderem Branche, Unternehmensgröße und gesetzliche Kriterien.

IT-SERVICE

buschkamp
Kompetent fürs Büro

NIS-2: Wer ist betroffen und welche Pflichten entstehen?

Die Europäische Union hat mit der zweiten Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) die Anforderungen an den Schutz digitaler Infrastrukturen deutlich erweitert. Die Richtlinie wurde im Dezember 2022 veröffentlicht und trat im Januar 2023 in Kraft. Ziel ist es, Unternehmen und Organisationen besser gegen Cyberangriffe und digitale Sicherheitsrisiken zu schützen.



Die EU-Mitgliedstaaten waren aufgefordert, die neuen Vorgaben bis Oktober 2024 in nationales Recht zu übertragen. Damit wurde der bisherige europäische Rechtsrahmen aus dem Jahr 2016 grundlegend weiterentwickelt.

WEN BETRIFFT NIS-2 UND WAS ÄNDERT SICH?

Mit NIS-2 wird der Kreis der betroffenen Unternehmen erheblich vergrößert. Neben besonders wichtigen Einrichtungen können nun auch zahlreiche weitere mittelständische Unternehmen unter die gesetzlichen Vorgaben fallen. Eine Rolle spielen dabei insbesondere die Branche, die Anzahl der Beschäftigten und der Jahresumsatz.

Betroffene Unternehmen müssen umfassende Sicherheitsmaßnahmen umsetzen. Dazu zählen ein strukturiertes Risikomanagement, sichere Lieferketten, Notfallkonzepte, Zugriffskontrollen und verbindliche Meldeverfahren bei Sicherheitsvorfällen.

Auch die Geschäftsführung trägt mehr Verantwortung für die Umsetzung und Überwachung der IT-Sicherheitsmaßnahmen. Bei Verstößen gegen die gesetzlichen Anforderungen können empfindliche Bußgelder drohen.

WAS VIELE UNTERNEHMEN NOCH NICHT WISSEN:

NIS-2 nimmt auch die Unternehmensleitung stärker in die Pflicht. Geschäftsführer müssen sich aktiv mit der IT-Sicherheit beschäftigen und an entsprechenden Schulungen teilnehmen. Je nach Einstufung des Unternehmens können sie bei Pflichtverletzungen persönlich zur Verantwortung gezogen werden.



IT-Sicherheit ist damit nicht mehr nur eine technische Aufgabe der IT-Abteilung, sondern eine zentrale Verantwortung der gesamten Unternehmensführung.

buschkamp
Kompetent fürs Büro

IT-SERVICE

Zertifizierungen und IT-Sicherheitsstandards

Der Schutz vertraulicher Informationen ist für Unternehmen heute wichtiger denn je. Kundendaten, interne Dokumente und geschäftliche Informationen müssen zuverlässig vor unbefugtem Zugriff geschützt werden. Anerkannte Zertifizierungen und internationale Standards helfen dabei, einheitliche Sicherheitsanforderungen zu definieren und deren Einhaltung nachvollziehbar zu machen.

SICHERHEIT BRAUCHT KLARE STANDARDS

Ein professionelles IT-Sicherheitskonzept beginnt mit der systematischen Erfassung möglicher Risiken. Dazu gehören die Überprüfung technischer Systeme, der Schutz sensibler Daten und die regelmäßige Kontrolle bestehender Sicherheitsmaßnahmen.

Besondere Bedeutung haben dabei internationale ISO-Normen:

- **ISO 9001** – Qualitätsmanagement: Definiert Anforderungen an strukturierte Prozesse und eine kontinuierliche Verbesserung der Qualität.
- **ISO 14001** – Umweltmanagement: Unterstützt Unternehmen dabei, Umweltbelastungen zu reduzieren und Ressourcen verantwortungsvoll einzusetzen.
- **ISO 27001** – Informationssicherheitsmanagement: Legt Anforderungen für den systematischen Schutz von Informationen und IT-Systemen fest.



Auch bei Druck- und Multifunktionssystemen spielt Datensicherheit eine wichtige Rolle. Moderne Sicherheitsfunktionen können Dokumente bereits während der Verarbeitung verschlüsseln und vor unbefugtem Zugriff schützen.

BUSCHKAMP – SICHERHEIT MIT SYSTEM

Wir unterstützen Unternehmen bei der Auswahl geeigneter Hard- und Software sowie moderner Sicherheitslösungen. Dabei stehen der Schutz Ihrer Daten, zuverlässige Technik und eine auf Ihre Anforderungen abgestimmte IT-Infrastruktur im Mittelpunkt.

Unser Anspruch:

Mehr Sicherheit, mehr Transparenz und ein gutes Gefühl bei der täglichen Arbeit mit Ihrer IT.

IT-SERVICE

buschkamp
Kompetent fürs Büro

Sicher mit der Cloud verbunden – Datenschutz hat Priorität



Cloud-Dienste erleichtern den Zugriff auf Unternehmensdaten und ermöglichen flexibles Arbeiten von nahezu jedem Standort. Voraussetzung dafür ist eine zuverlässige Absicherung der Datenübertragung. Denn nicht nur die Speicherung, sondern auch der Weg zwischen dem eigenen Unternehmen und der Cloud muss vor unbefugten Zugriffen geschützt sein.

Sicherheit beginnt bereits bei der Datenübertragung. Moderne Verschlüsselungsverfahren wie TLS schützen Informationen während der Übermittlung. Ergänzende Verschlüsselungstechnologien sorgen dafür, dass gespeicherte Daten auf Festplatten und SSDs ebenfalls geschützt bleiben.

DREI WICHTIGE BAUSTEINE FÜR MEHR DATENSICHERHEIT:

SICHERE CLOUD-ANBINDUNG

Professionelle Cloud-Lösungen ermöglichen einen geschützten Zugriff auf Unternehmensdaten. Achten Sie bei der Auswahl auf geeignete Sicherheitsstandards, nachvollziehbare Zertifizierungen und eine DSGVO-konforme Datenverarbeitung. Auch mobile Drucklösungen und digitale Zeiterfassung sollten über abgesicherte Verbindungen erfolgen.

DATEN SICHER UND DAUERHAFT LÖSCHEN

Gehen Geräte verloren oder werden ausgemustert, müssen darauf gespeicherte vertrauliche Informationen zuverlässig entfernt werden. Professionelle Löschverfahren verhindern, dass Daten später wiederhergestellt werden können. Je nach Anforderung kommen hierfür unterschiedliche zertifizierte Verfahren zum Einsatz.

DATENSCHUTZ NACH DSGVO

Der Umgang mit personenbezogenen Daten unterliegt klaren gesetzlichen Vorgaben. Unternehmen müssen sicherstellen, dass vertrauliche Informationen geschützt verarbeitet, gespeichert und übertragen werden. Ein durchdachtes Datenschutz- und Sicherheitskonzept hilft, Risiken zu minimieren und gesetzliche Anforderungen einzuhalten.



SICHERE CLOUD-ANBINDUNG

Achten Sie bei der Auswahl auf anerkannte Sicherheitsstandards und eine DSGVO-konforme Datenverarbeitung. So greifen Sie sicher auf Ihre Daten in der Cloud zu.



DATENSCHUTZ NACH DSGVO

Vertrauliche Informationen müssen bei der Entsorgung von Geräten oder Dateien zuverlässig entfernt werden durch professionelle Löschverfahren.



DATEN SICHER UND DAUERHAFT LÖSCHEN

Stellen Sie sicher, dass personenbezogene Daten nach den gesetzlichen Vorgaben geschützt verarbeitet, gespeichert und übertragen werden.

buschkamp
Kompetent fürs Büro

IT-SERVICE

Schwachstellen aufdecken und Sicherheitslücken schließen

Jedes IT-System kann Schwachstellen aufweisen. Umso wichtiger ist es, mögliche Risiken frühzeitig zu erkennen und gezielt zu beseitigen. Buschkamp unterstützt Unternehmen dabei, ihre IT- und Druckinfrastruktur sicherer zu gestalten – von der passenden technischen Ausstattung bis hin zu individuellen Sicherheitslösungen.

Besonders Drucker und Multifunktionsgeräte werden bei der IT-Sicherheit häufig unterschätzt. Beim Drucken, Kopieren und Scannen entstehen digitale Daten, die teilweise auf internen Festplatten oder im Zwischenspeicher abgelegt werden. Diese Informationen müssen zuverlässig vor fremdem Zugriff geschützt sein. Eine einfache Löschung reicht dabei nicht immer aus. Durch geeignete Verfahren zur sicheren Datenüberschreibung lässt sich verhindern, dass vertrauliche Dokumente später wiederhergestellt werden können.

Sicherheit bedeutet auch, potenzielle Schwachstellen rechtzeitig aufzuspüren. Regelmäßige Überprüfungen der Systeme helfen dabei, Sicherheitsrisiken zu erkennen und geeignete Gegenmaßnahmen einzuleiten. Auf dieser Grundlage lassen sich Schutzkonzepte entwickeln, die zur technischen Ausstattung und den Anforderungen des jeweiligen Unternehmens passen.



IT-SYSTEME UND DRUCKERFLOTTEN IM BLICK BEHALTEN

Eine kontinuierliche Überwachung schafft Transparenz und hilft, ungewöhnliche Aktivitäten frühzeitig zu erkennen. Moderne Softwarelösungen ermöglichen die zentrale Kontrolle von Druckaufträgen, Geräteauslastung und Benutzerrechten. Ergänzend sorgen regelmäßige Firmware-Updates dafür, dass bekannte Sicherheitslücken geschlossen und Systeme auf einem aktuellen Stand gehalten werden.

Unser Ziel:

Mehr Kontrolle, weniger Sicherheitsrisiken und eine zuverlässige IT-Infrastruktur für Ihren Arbeitsalltag.

Updates und Firmware – Technik auf dem neuesten Stand

Drucker und Multifunktionssysteme sind längst ein fester Bestandteil der betrieblichen IT-Infrastruktur. Deshalb benötigen auch diese Geräte regelmäßige Sicherheitsaktualisierungen. Veraltete Firmware und fehlende Updates können Einfallstore für Cyberangriffe sein. Umso wichtiger ist es, Sicherheitsupdates zeitnah einzuspielen und die Geräte technisch aktuell zu halten.

Die Lösung:
Regelmäßige Wartung und automatisierte Aktualisierungen. Moderne Drucksysteme bieten verschiedene Sicherheitsfunktionen, um Manipulationen und unbefugte Eingriffe zu verhindern. Dazu gehören beispielsweise geschützte Startvorgänge und automatische Integritätsprüfungen. Werden Veränderungen an der Firmware festgestellt, können entsprechende Schutzmechanismen



Regelmäßige Schulungen – Sicherheit beginnt beim Menschen

Die beste technische Absicherung kann nur dann zuverlässig funktionieren, wenn auch die Mitarbeiterinnen und Mitarbeiter für mögliche Gefahren sensibilisiert sind. Unachtsamkeit, unsichere Passwörter oder ein unbedachter Klick auf einen unbekannten Link können erhebliche Sicherheitsrisiken verursachen.

Deshalb gehört die regelmäßige Aufklärung der Belegschaft zu einem umfassenden IT-Sicherheit-skonzept. Mitarbeiter sollten wissen, wie sie verdächtige E-Mails erkennen, mit vertraulichen Informationen umgehen und mögliche Bedrohungen richtig einschätzen.

Denn IT-Sicherheit ist Teamarbeit. Wenn moderne Technik und geschulte Mitarbeiter zusammenspielen, lassen sich viele Risiken bereits im Vorfeld vermeiden.



buschkamp
Kompetent fürs Büro

IT-SERVICE

Plus: IT-SICHERHEITS-CHECKLISTE

Wie gut ist Ihre Drucker- und IT-Infrastruktur tatsächlich geschützt?

Prüfen Sie anhand dieser Fragen, ob Sie die wichtigsten Sicherheitsmaßnahmen in Ihrem Unternehmen bereits umgesetzt haben.

- Haben Sie voreingestellte Passwörter durch sichere, individuelle Zugangsdaten ersetzt?
- Ist sichergestellt, dass sich Nutzer vor der Verwendung von Multifunktionsgeräten authentifizieren müssen?
- Setzen Sie eine Mehr-Faktor-Authentifizierung für wichtige Zugänge und Anwendungen ein?
- Sind Ihre Netzwerkeinstellungen auf die Sicherheitsanforderungen Ihres Unternehmens abgestimmt?
- Werden Sicherheitsupdates und Firmware-Aktualisierungen zeitnah installiert?
- Kontrollieren Sie regelmäßig, ob die Firmware Ihrer Druck- und Multifunktionssysteme unverändert und sicher ist?
- Erfolgt die Kommunikation mit Cloud-Diensten über ausreichend abgesicherte Verbindungen?
- Verwenden Sie aktuelle Verschlüsselungsverfahren für die Übertragung und Speicherung sensibler Daten?
- Ist gewährleistet, dass gelöschte Daten auf Festplatten nicht wiederhergestellt werden können?
- Erfüllen Ihre IT-Sicherheitsmaßnahmen die relevanten Anforderungen von DSGVO und NIS-2?
- Sind Benutzerrechte und Administratorzugänge für Ihre Druckerflotte eindeutig geregelt?
- Werden Ihre Mitarbeiter regelmäßig über Sicherheitsrisiken im Umgang mit Drucksystemen informiert?
- Finden wiederkehrende Schulungen statt, um den sicheren Umgang mit IT-Anwendungen zu vermitteln?

Sie haben nicht alle Fragen mit Ja beantworten können?

Dann ist es Zeit, Ihre IT-Sicherheit genauer unter die Lupe zu nehmen. Buschkamp unterstützt Sie dabei, mögliche Schwachstellen zu erkennen und passende Lösungen zu finden.
Sprechen Sie mit uns. Gemeinsam machen wir Ihre IT und Druckerflotte sicherer.

buschkamp
Kompetent fürs Büro

Technik, Möbel, Service. Alles aus einer Hand.

Fazit

IT-Sicherheit ist eine Investition in die Zukunft

Sicherheitslücken in der IT können erhebliche Schäden verursachen. Unternehmen, die auf moderne Schutzkonzepte setzen, ihre Systeme regelmäßig aktualisieren und Cloud-Anwendungen zuverlässig absichern, schaffen eine wichtige Grundlage, um Cyberangriffen wirksam entgegenzuwirken.

Dabei gilt: IT-Sicherheit ist keine einmalige Maßnahme, sondern muss kontinuierlich weiterentwickelt werden. Neben der passenden technischen Ausstattung sind regelmäßige Kontrollen und gut geschulte Mitarbeiter entscheidend. Nur wenn alle Bereiche zusammenspielen, lassen sich Risiken dauerhaft reduzieren und sensible Unternehmensdaten wirksam schützen.

Auch Drucker, Kopierer und Multifunktionssysteme müssen dabei berücksichtigt werden. Moderne Geräte verfügen über umfangreiche Sicherheitsfunktionen, die dazu beitragen, vertrauliche Informationen zu schützen und unbefugte Zugriffe zu verhindern. Durch die richtige Konfiguration und Einbindung in das Unternehmensnetzwerk lassen sich zusätzliche Sicherheitsrisiken vermeiden und Datenschutzanforderungen besser erfüllen.

Buschkamp unterstützt Sie dabei, Ihre IT- und Druckerumgebung sicher aufzustellen. Von der Auswahl geeigneter Systeme über die Einrichtung bis hin zur laufenden Betreuung stehen wir Ihnen mit Erfahrung und passenden Lösungen zur Seite.

Denn zuverlässige IT-Sicherheit beginnt bei der richtigen Technik – und hört beim Service nicht auf.







Buschkamp – Technik, Möbel, Service. Alles aus einer Hand.