Mai | Juni 2022

cosoft

Ihr IT-Systempartner – seit 1985

Phishing:
Damit müssen Sie rechnen!

Sicherer arbeiten:
mit Ihrem IT-Dienstleister!

Cybercrime auf dem Höchststand

Schützen Sie Ihr Unternehmen!

Cybercrime auf dem Höchststand.

Schützen Sie Ihr Unternehmen!

Nichts ist sicher. Das haben uns die vergangenen Monate bewiesen. Spätestens seit dem russischen Angriffskrieg auf die Ukraine am 24. Februar 2022 können wir uns dessen gewiss sein. Denn tatsächlich gerechnet hat damit wohl kaum jemand. Seitdem werden wir begleitet von Sorgen – menschlicher, aber auch wirtschaftlicher Natur.

Längst ist klar: Der Schauplatz des Krieges bekommt durch das World Wide Web ein völlig anderes Ausmaß, das für Unternehmen auf der ganzen Welt bedrohlich werden kann. Dabei begann die russische Offensive schon einige Zeit vorher mit Angriffen im digitalen Raum und wird – je länger der Krieg in der Ukraine dauert – wohl auch weiterhin Kriegsschauplatz bleiben.

Was bedeutet das für Unternehmen? Mit welchen Angriffen muss gerechnet werden und wie können sich Firmen wappnen? Auf diese Fragen möchten wir Antworten liefern und Ihnen zeigen, wie Sie sich schützen können.

Offizielle Stellen bestätigen Gefahr

Ganz gleich, ob BSI (Bundesamt für Sicherheit in der Informationstechnik), Bitkom (Branchenverband der deutschen Informations- und Telekommunikationsbranche) oder ACS (Allianz für Cybersicherheit): Die Cybersicherheitsexperten in Deutschland sind sich einig, dass der russische Angriff auf die Ukraine die Gefahr im Netz deutlich erhöht. Der einschlägige Rat lautet daher, ruhig und wachsam zu bleiben, aber auch, sich kompetente IT-Unterstützung zu holen.

Tatsache ist nämlich: So sehr wir die Vorteile des Internets in den vergangenen Jahrzehnten zu schätzen gelernt haben, so verwundbar machen sie uns heutzutage.

Hacking-Angriffe: Damit ist zu rechnen

Bereits Anfang März warnte das Bundesamt für Verfassungsschutz vor der Gruppierung »Ghostwriter«, einer Hacker-Gruppe des russischen Geheimdienstes. Diese verübte zielgerichtet Angriffe auf kritische Infrastrukturen (zum Beispiel Kraft- und Wasserwerke), was wohl als Reaktion auf die Sanktionen gegen Russland zu werten ist. Mit welchen Angriffstypen ist zu rechnen?

DDos-Attacken

DDos-Attacken zielen darauf ab, mit gezielten Angriffen ein ungeschütztes System lahmzulegen. Durch gezielte Attacken werden Dienste oder Server derart stark frequentiert, dass sie überlasten und ausfallen. Durch den Systemausfall können Unternehmen nicht weiterarbeiten und ein finanzieller Schaden entsteht.

Wiper-Attacken

Wiper-Attacken richten im Gegensatz zu DDos-Angriffen einen bleibenden Schaden an. Das Ziel: Daten, die auf Festplatten sind, dauerhaft zu vernichten.

Defacement bzw. Fake News

Dass man längst nicht allen Nachrichten glauben darf, die derzeit berichtet werden, ist jedem klar. Beim Defacement ist es aber gar nicht so einfach, Fake News zu identifizieren. Hacker-Gruppen übernehmen dabei ganze Internetseiten und können dort irreführende Inhalte veröffentlichen, die gar nicht so abwegig erscheinen. Im schlimmsten Fall würden diese Nachrichten dann selbst von renommierten Nachrichten-Agenturen für bare Münze gehalten und weiter verbreitet.

So schützen Sie sich

Grundsätzlich gilt, die Schutzmaßnahmen insgesamt zu verstärken.

- ✔ Achten Sie auf aktuelle Betriebssysteme und Software und spielen Sie die neuesten Sicherheitsupdates so schnell wie möglich ein.
- ✔ Verwenden Sie sichere Passwörter. Sie sollten sowohl komplex als auch unterschiedlich sein. Geben Sie diesen Ratschlag auch dringend an Ihre Mitarbeiter weiter und nutzen Sie am besten einen Passwort-Manager.
- ✔ Nutzen Sie die Multi-Faktor-Authentifizierung bei allen Logins mit Außenanbindung.
- ✔ Definieren Sie die Benutzerrechte Ihrer Mitarbeiter und entziehen Sie ihnen (wenn möglich) Administrator-Rechte, die sie nicht benötigen.
- ✔ Überprüfen Sie Ihre Backup-Strategie. Sind Ihre wichtigen Unternehmensdaten geschützt und gesichert?

Wir helfen Ihnen!

Sie sehen Handlungsbedarf bei sich im Unternehmen? Dann kontaktieren Sie uns. Wir haben die notwendige Expertise und kennen auch den richtigen Hebel, um die Gefahr, Opfer eines Cyber-Angriffs zu werden, für Ihr Unternehmen zu reduzieren. Mehr zu diesem Thema erfahren Sie übrigens auf Seite fünf dieser Ausgabe.

Sprechen Sie uns an!

Phishing: Damit müssen Sie rechnen!

»Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten.«

Etwas hoch gegriffen? Nein, denn das, was General Sunzi in seinem Buch »Die Kunst des Krieges« bereits um 500 vor Christus niederschrieb, lässt sich durchaus auch auf Cyberkriminalität übertragen. Die Wahrheit ist: Je besser Sie wissen, mit welchen Methoden Cyberkriminelle in Ihr Netzwerk kommen wollen, desto besser sind Sie davor gefeit.

Social Engineering: So sehen Angriffe aus

Bestimmt haben Sie schon einmal von Phishing gehört. Grob zusammengefasst geht es darum, dass Cyberkriminelle zum Beispiel über Spam-Mails, Direktnachrichten (etwa SMS), fingierte Webseiten, Profile oder Anrufe versuchen, an persönliche Daten zu kommen. Besonders fies: Die Angriffe sind mittlerweile so gut getarnt, dass nichtsahnende Empfänger die Nachrichten ohne böse Hintergedanken öffnen (beispielsweise angehängte Dateien in einer Bewerbungsmail an Personaler). Schon haben Sie den Eindringling in Ihrem Netzwerk.

Phishing und das Geschäft mit dem Krieg

Phishing-Mails sind ein alter Hut und sicher kein Neuland für Sie und Ihre Mitarbeiter. Neu ist jedoch der Bezug zum Ukraine-Krieg. In aktuellen Phishing-Mails könnten Sie beispielsweise dazu aufgefordert werden, Kriegsopfern schnell Geldmittel zur Verfügung zu stellen, um eine Flucht zu ermöglichen. Achten Sie ebenso auf reißerische E-Mails oder Nachrichten, die durch Klicken auf den Weiterlesen-Button Schadsoftware auf Ihren Rechner laden. Ebenso gefährlich können Scam-Mails sein, die betrügerische Spendenaufrufe verteilen.

Im Fadenkreuz Cyberkrimineller

Social-Engineering-Angriffe richten sich direkt gegen Menschen, die nicht ausreichend geschützt oder sensibilisiert worden sind. Der Grund dafür ist oftmals Unkenntnis, denn häufig schulen Unternehmer ihre Mitarbeiter nicht oder nicht ausreichend vor den Gefahren und deren Formen im Internet.

Tun Sie sich und Ihrem Unternehmen einen Gefallen und seien Sie wachsam. Lassen Sie sich nicht vorschnell zu einer Handlung bewegen, die Ihnen möglicherweise das Handwerk legt. Handeln Sie überlegt, hinterfragen Sie kritisch und sensibilisieren Sie auch Ihre Mitarbeiter. Die Cyber-Bedrohungslage – da sind sich Experten einig – wird sich sehr wahrscheinlich nicht kurzfristig entspannen.

Sicherer arbeiten: mit Ihrem IT-Dienstleister!

Nun kennen Sie die Cyber-Bedrohung, die durch den Ukraine-Krieg auch deutsche Unternehmen gefährdet. Sind Sie gewappnet oder müssen Sie in einigen Belangen noch Ihre digitalen Hausaufgaben machen?

Nur sicher mit kontinuierlichen Maßnahmen

Ihre IT steht aktuell auf sicheren Füßen? Das ist gut. Viel wichtiger ist aber, dass sie das auch bleibt. Regelmäßige Updates aller eingesetzter Software, umfangreiche Backups Ihrer Daten, ein Antivirus- oder Firewall-Management sowie viele weitere Maßnahmen bringen Sie einem gut geschützten System ein gutes Stück näher. Doch zu Recht fragen Sie sich jetzt sicher: Wie soll das neben allen anderen Aufgaben in Ihrem Arbeitsalltag bewerkstelligt werden? Die Lösung ist einfach: durch Managed Services und einen kompetenten IT-Dienstleister an Ihrer Seite.

Managed Services: Die Antwort auf Ihre Fragen

Managed Service kann man ungefähr mit Rundum-sorglos-Service übersetzen. Damit liefert Ihnen Ihr IT-Dienstleister für eine monatlich feste Service-Pauschale die entscheidenden Mehrwerte, damit Sie unbeschwert, effizient und ohne böse Überraschungen arbeiten können. Für Sie bedeutet Managed Services also zweierlei: kalkulierbare Kosten und eine verlässliche IT.

Ihr IT-Dienstleister oder auch Managed Services Provider (kurz MSP) genannt, nimmt Ihnen dabei die Sorgen um bestimmte IT-Bereiche oder sogar Ihre gesamte IT ab. Mit dem entsprechenden Managed-Service-Paket sorgt er nicht nur für einen reibungslosen Arbeitsablauf ohne Komplikationen. Er kann auch sicherstellen, dass Cyberkriminelle es schwerer haben, in Ihr Netzwerk einzudringen und Ihr Geschäft möglicherweise sogar irreversibel zu schädigen.

Durch Managed Services entscheiden Sie sich also proaktiv gegen Systemausfälle und andere kleinere Probleme, die ansonsten Ihren Arbeitsalltag und den Ihrer Mitarbeiter behindern könnten, decken aber auch wichtige Sicherheitsaspekte ab.

Ihre IT? Läuft – mit Managed Services!

Als Ihr erfahrener IT-Dienstleister empfehlen wir kleinen und mittleren Unternehmen den Einsatz von Managed Services. Lassen Sie sich von uns kompetent beraten!

Gern ermitteln wir gemeinsam mit Ihnen Ihren individuellen Bedarf und können Ihnen anschließend die passenden Managed Services empfehlen, damit Sie sich – nicht nur in Anbetracht der aktuellen Entwicklungen – sicherer fühlen.

Sprechen Sie uns an!

Zuverlässige Partner für die alltäglichen Aufgaben

HP 250 G8 SP

Intel® Core™ i5-1135G7 Prozessor (bis zu 4,20 GHz mit Intel® Turbo-Boost-Technik 2.0, 8 MB Intel® Cache) | 8 GB RAM | 256 GB SSD | Intel® Iris Xe Grafik | Card-Reader Schnittstellen u. a. HDMI, USB, USB-C, LAN | Windows 10 Pro – kostenloses Upgrade auf Windows 11* | 1 Jahr Herstellergarantie**

419,00
zzgl. gesetzl. USt.

HP ProBook 450 G8

Intel® Core™ i5-1135G7 Prozessor (bis zu 4,20 GHz mit Intel® Turbo-Boost-Technik 2.0, 8 MB Intel® Cache) | 16 GB RAM | 1 TB SSD | Intel® Iris Xe Grafik | Card-Reader Schnittstellen u. a. HDMI, USB, DisplayPort-Unterstützung über USB-C, LAN | Tastatur mit Hintergrundbeleuchtung | Fingerprint-Reader | Windows 10 Pro – kostenloses Upgrade auf Windows 11* | 1 Jahr Herstellergarantie**

879,00
zzgl. gesetzl. USt.

HP E24 G4

Auflösung 1.920 x 1.080 Pixel im 16:9-Format bei 60 Hz | Kontrast: 1.000:1 Helligkeit 250 cd/m² | Reaktionszeit 5 ms | HDMI, DisplayPort, VGA, USB 3 Jahre Herstellergarantie**

195,00
zzgl. gesetzl. USt.

*Der Zeitpunkt des Upgrades kann je nach Gerät variieren. Features und App-Verfügbarkeit können je nach Region variieren. Bestimmte Features erfordern spezielle Hardware (siehe »aka.ms/windows11-spezifikationen«). | **Die zusätzliche Garantie schränkt die gesetzliche Gewährleistung von 24 Monaten nicht ein. Garantie-Erweiterung gegen Aufpreis möglich.

Bestens ausgestattet für Ihr Business

2,7"-TOUCHSCREEN

AIRPRINT-FÄHIG

Canon

CANON Maxify GX6050 3in1

3-in-1-Tintenstrahldrucker – drucken, scannen, kopieren | Druckauflösung bis zu 600 x 1.200 dpi | Druckgeschwindigkeit bis zu 24 Seiten/Minute in S/W, bis zu 15,5 Seiten/Minute in Farbe | Monatliche Druckleistung von bis zu 45.000 Seiten | Papierzufuhrkapazität 350 Blatt | Automatischer Duplexdruck | USB, LAN, Wi-Fi

409,00

zzgl. gesetzl. USt.

LÖSUNG FÜR DIE UNTERBRECHUNGSFREIE STROMVERSORGUNG VON NETZWERKGERÄTEN

AKUSTISCHER ALARM BEI BATTERIEBETRIEB UND ÜBERLASTUNGSALARM

Life Is On APC by Schneider Electric

APC USV Smart-UPS

Leistungskapazität: 700 Watt/1.000 VA | Anschlüsse: 8 x Strom IEC 60320 C13, 2 x IEC-Jumper | Übertragungszeit: 6 ms | Batterieaustausch möglich | Nur 3 Stunden Ladezeit | 3 Jahre Herstellergarantie*

469,00

zzgl. gesetzl. USt.

Nicht das Passende gefunden? Fragen Sie uns nach einem Angebot für Ihre individuellen unternehmerischen Anforderungen!

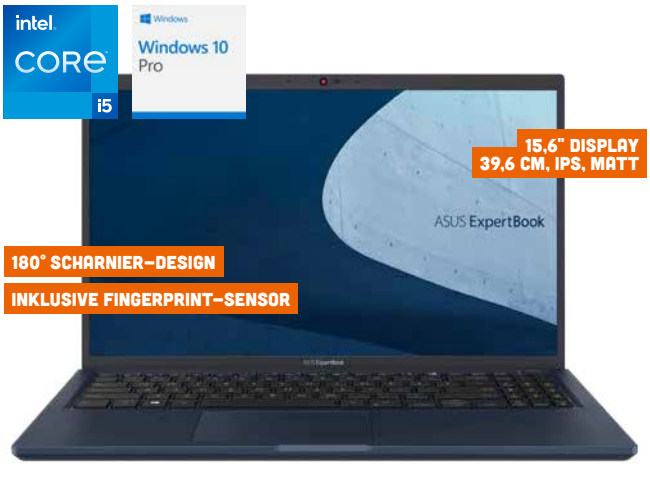
DELL

DELL Latitude 3520

Intel® Core i5-1135G7 Prozessor (bis zu 4,20 GHz mit Intel® Turbo-Boost-Technik 2.0, 8 MB Intel® Cache) | 8 GB RAM | 256 GB SSD | Intel® Iris Xe Grafik | Card-Reader Schnittstellen u. a. HDMI, USB, USB-C, LAN | Fingerprint-Reader | Tastatur mit Hintergrundbeleuchtung | Windows 10 Pro – kostenloses Upgrade auf Windows 11* 1 Jahr Herstellergarantie**

699,00

zzgl. gesetzl. USt.



ASUS

ASUS ExpertBook B1

Intel® Core i5-1135G7 Prozessor (bis zu 4,20 GHz mit Intel® Turbo-Boost-Technik 2.0, 8 MB Intel® Cache) | 16 GB RAM | 512 GB SSD | Intel® Iris Xe Grafik | Card-Reader Schnittstellen u. a. HDMI, USB, VGA, Thunderbolt, LAN | Tastatur mit Hintergrundbeleuchtung | Windows 10 Pro – kostenloses Upgrade auf Windows 11* 1 Jahr Herstellergarantie**

739,00

zzgl. gesetzl. USt.

Windows 11 ist ein modernes und zugleich vertrautes Betriebssystem für einen fokussierten und reibungslosen Arbeitsalltag. Eine übersichtliche, eingängige Bedienoberfläche fördert die Produktivität und vereinfacht das zielgerichtete Arbeiten. App-Kompatibilität und Cloud-Verwaltung erleichtern die Einführung. Ein Betriebssystem, das Zero Trust unterstützt, sorgt für mehr Sicherheit – ganz gleich, wo Sie das Berufsleben hinführt. Die produktivste und sicherste Version von Windows – und dennoch einfach für die IT.

Auf einen Blick:

- Frischer Wind: Windows 11 ist auf hybrides Arbeiten und mobile Geräte ausgelegt
- Windows 11 erstrahlt im neuen Look, ist im Netzwerk aber wie Windows 10 zu handhaben
- Im Fokus: mehr Sicherheit durch Systemanforderungen und Konsistenz für die IT
- Microsoft 365 – der perfekte Begleiter für Windows 11 und hybrides Arbeiten
- Windows 10 erhält weiterhin Support, sodass für den Umstieg ausreichend Zeit bleibt

Fujitsu empfiehlt Windows 11 Pro für Unternehmen

Fujitsu Lifebook A3511

Intel® Core i5-1135G7 Prozessor (bis zu 4,20 GHz mit Intel® Turbo-Boost-Technik 2.0, 4 MB Intel® Cache) | Windows 11 Pro | 8 GB RAM | 256 GB SSD | Intel® Iris Xe Grafik | DVD±RW Card-Reader | Schnittstellen u. a. HDMI, USB, DisplayPort-Unterstützung über USB-C, LAN
1 Jahr Herstellergarantie**

629,00
zzgl. gesetzl. USt.

Stand 05/2022. Gültig bis 30. Juni 2022. Solange der Vorrat reicht. Irrtümer und Preisänderungen vorbehalten. Alle Preise sind Euro-Preise zzgl. gesetzl. USt.
Bildnachweise Adobe Stock: # 188725063 © fergregory; # 448296145 © James Thew; # 266056885 © pickup; # 178545871 © pickup

cosoft
Ihr IT-Systempartner – seit 1985

cosoft computer consulting gmbh | Borkener Str. 134a | 48653 Coesfeld
Telefon +49 2541 94750 | Fax +49 2541 947590 | E-Mail info@cosoft.de
Internet https://www.cosoft.de