Ratgeber des JOBSTARTER plus-Projekts
KUKUDI
Kunststoff.KMU.Umbruch.Digitalisierung

IT-Sicherheit in KMU

GEFÖRDERT VOM
Gefördert als JOBSTARTER plus-Projekt aus Mitteln des Bundesministeriums für Bildung und Forschung und des Europäischen Sozialfonds.

IT-Sicherheit im unternehmerischen Fokus

Die Coronapandemie hat die Digitalisierung der Wirtschaft nachhaltig beschleunigt. Home-Office, Videokonferenzen und Cloud-Lösungen haben im Zuge dessen außerdem dafür gesorgt, dass dem Themenkomplex IT-Sicherheit mehr und mehr Aufmerksamkeit zuteilwird. Das verstärkte Bewusstsein für dieses unternehmerische Handlungsfeld lässt sich anhand eines beeindruckenden Trends veranschaulichen: Nach einer aktuellen Studie des Digitalverbands Bitkom soll der Umsatz mit Hardware, Software und Services im Bereich der IT-Sicherheit bis zum Ende des Jahres 2021 auf 6,2 Milliarden Euro ansteigen. Damit wird dieser Wert den bisherigen Rekord aus dem Vorjahr 2020 (5,6 Milliarden Euro) nochmals um fast zehn Prozent übertreffen.

Insbesondere kleine und mittelständische Unternehmen kommen in der heutigen Zeit nicht umhin, sich mit der Sicherheit ihrer eigenen IT-Systeme fundiert auseinanderzusetzen sowie bisherige Prozesse zu hinterfragen und – falls nötig – zu optimieren. Denn die Zeit drängt: Der DsiN-Praxisreport „Mittelstand IT-Sicherheit 2020“ zeigte, dass fast die Hälfte der befragten Unternehmen im Befragungszeitraum zwischen April 2019 und April 2020 Opfer einer Cyberattacke wurden.

Auf den nachfolgenden Seiten haben wir alles Wissenswerte rund um das Thema IT-Sicherheit für Sie zusammengestellt.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Zusammen. Zukunft. Gestalten.
Gefördert als JOBSTARTER plus-Projekt aus Mitteln des Bundesministeriums für Bildung und Forschung und des Europäischen Sozialfonds.

Vorbereitung

Ein erster wichtiger Arbeitsschritt zum Aufbau einer nachhaltigen IT-Sicherheitsinfrastruktur ist die klare Zuordnung von Verantwortlichkeiten. Es bedarf unbedingt einer oder mehrerer Mitarbeiter*innen, die sich hauptverantwortlich um Belange der IT-Security sowie das Notfallmanagement kümmern. Sodann können in Abstimmung mit Ihrem IT-Dienstleister Erstmaßnahmen bei sicherheitsrelevanten IT-Vorfällen definiert werden. Dies betrifft beispielsweise die Festlegung eines geregelten Vorgehens und die Definition fester Alarmierungs- und Entscheidungswege in einer solchen Situation. Auch eine entsprechende Krisenkommunikation, die externe (Presse, Öffentlichkeit) und interne (Mitarbeiter*innen) Zielgruppen gleichermaßen berücksichtigt, sollte gleich zu Beginn aufgesetzt werden.

Ein fester Bestandteil der Vorbereitungsphase ist weiter eine umfassende Prüfung der bestehenden IT-Infrastruktur. Dabei sind insbesondere folgende Punkte zu berücksichtigen:

- Vergeben Sie restriktive Benutzerrechte an Ihren Systemen.
- Lassen Sie Ihre IT-Infrastruktur regelmäßig auf Angreifbarkeit prüfen.
- Installieren Sie aktive Überwachungsmaßnahmen (Monitoring) für Ihre IT-Landschaft, jedoch ohne dabei den Datenschutz zu vernachlässigen.
- Führen Sie regelmäßig Übungen für IT-Notfälle durch, bei denen der Ernstfall – etwa eine Cyberattacke – unter Realbedingungen simuliert wird.
- Installieren Sie regelmäßig und unverzüglich Patches und Sicherheitsupdates.
- Setzen Sie Programme zum Schutz vor Schadsoftware ein und aktualisieren Sie diese regelmäßig.
- Nutzen Sie Firewalls, um Ihre Netze und Rechner vor Angriffen von außen zu schützen.
- Erstellen Sie regelmäßig Sicherheitskopien (Backups) Ihrer Daten, und testen Sie regelmäßig deren Wiederherstellung.
- Dokumentieren Sie Ihre IT-Infrastruktur, beispielsweise mittels eines Netzplans oder einer IP-Dokumentation.
- Segmentieren Sie Ihr Netzwerk.
- Prüfen Sie, ob eine Dokumentation beispielsweise nach ISIS12 sinnvoll ist. Durch eine detaillierte Dokumentation werden potenzielle Schwachstellen sichtbar.

GEFÖRDERT VOM
jobstarter Für die Zukunft ausbilden
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
Europäische Union
Zusammen. Zukunft. Gestalten.
bibb Bundesinstitut für Berufsbildung

Gefördert als JOBSTARTER plus-Projekt aus Mitteln des Bundesministeriums für Bildung und Forschung und des Europäischen Sozialfonds.

Sensibilisierung / Bereitschaft

Die regelmäßige Sensibilisierung Ihrer Mitarbeiter*innen ist ein weiterer elementarer Schritt bei der Sicherstellung der IT-Sicherheit. Erstellen Sie daher zunächst eine Liste mit Ansprechpartner*innen und deren Erreichbarkeiten und stellen Sie diese der Belegschaft ebenso wie die Notfallrufnummern der IT-Abteilung zur Verfügung.

Beachten Sie darüber hinaus die nachstehenden Handlungsempfehlungen:

- Legen Sie verbindliche Regeln für die Vergabe und regelmäßige Änderung von Passwörtern fest.
- Passwörter sollten niemals für jedermann einsehbar – etwa auf einem Post-it am Monitor – am Arbeitsplatz aufbewahrt werden.
- Weisen Sie Ihre Mitarbeiter*innen außerdem darauf hin, ihre Computer auch bei kurzer Abwesenheit vom Arbeitsplatz zu sperren. Andernfalls besteht insbesondere in Großraumbüros die Gefahr, dass sich Unbefugte Zugang zu sensiblen Daten und Informationen verschaffen.

Bewältigung

Ist der sogenannte „Worst Case“ in Form eines IT-sicherheitsrelevanten Notfalls aufgetreten, zahlen sich die umfassenden Vorbereitungsmaßnahmen aus. Auch bei der Bewältigung einer solchen Sondersituation empfiehlt es sich, einem festen Ablaufplan mit klar definierten Handlungsanweisungen und Zuständigkeiten zu folgen. Darin sollten sich unter anderem die folgenden to Do’s wiederfinden:

- Identifikation von Art und Form des Auftretens der Infektion.
- Befragung betroffener Nutzer*innen zu Beobachtungen und Aktivitäten.
- Dokumentation von Sachverhalten, die mit dem Notfall in Zusammenhang stehen könnten.
- Sofortige Information aller Ansprechpartner*innen, die zur Bewältigung der Notfallsituation benötigt werden.

GEFÖRDERT VOM
Gefördert als JOBSTARTER plus-Projekt aus Mitteln des Bundesministeriums für Bildung und Forschung und des Europäischen Sozialfonds.

- Kontaktierung von IT-Dienstleistern, die bei der Bewältigung der Lage helfen können.
- Sammlung und Sicherung von Systemprotokollen, Logdateien und weiteren Daten.
- Meldung des Vorfalls bei den zuständigen Behörden (Polizei, Landesamt für Sicherheit in der Informationstechnik etc.).
- Beachtung von Meldepflichten.
- Kontaktierung der Verfassungsschutzbehörden, falls es sich beim Urheber der Cyberattacke um einen fremden Nachrichtendienst handeln könnte.

Nachbereitung

Ebenso wichtig wie die Vorbereitung möglicher Ernstfälle ist die Nachbereitung und Evaluation IT-sicherheitsrelevanter Ereignisse. Die nachstehenden Handlungsempfehlungen sollten bei diesem abschließenden Schritt ihre Berücksichtigung finden.

- Identifizieren Sie das „Sicherheitsleck“ und schließen Sie durch den IT-Notfall aufgedeckte Schwachstellen und Sicherheitslücken.
- Überwachen und Monitoren Sie Ihr Netzwerk und Ihre IT-Systeme.
- Überprüfen Sie bestehende Regelungen, Prozessen und Maßnahmen regelmäßig und optimieren Sie diese gegebenenfalls.
- Halten Sie Ihre Dokumentationen zum Notfallmanagement auf dem aktuellen Stand.
- Entwickeln Sie Ihre IT-Sicherheitsarchitektur weiter.
- Halten Sie sich permanent auf dem neusten Stand Ihrer Software Patches.
- Informieren Sie die Belegschaft über den Vorfall und sensibilisieren Sie Ihre Mitarbeiter*innen kontinuierlich zu Themen der IT-Sicherheit.
- Bleiben Sie wachsam.

Diese Informationen sind als Basis zur Entwicklung eines IT-Sicherheitskonzeptes zu verstehen. Detaillierte Informationen finden Sie auch auf den Seiten des zuständigen Landesamts für IT-Sicherheit.

Für weitere Informationen stehen wir Ihnen gerne zur Verfügung!

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Zusammen. Zukunft. Gestalten.

Gefördert als JOBSTARTER plus-Projekt aus Mitteln des Bundesministeriums für Bildung und Forschung und des Europäischen Sozialfonds.

KUKUDI
Kunststoff.KMU.Umbruch.Digitalisierung

Über KUKUDI:

Das JOBSTARTER plus-Projekt „KUKUDI – Kunststoff.KMU.Umbruch.Digitalisierung“ wird von den Beruflichen Fortbildungszentren der Bayerischen Wirtschaft (bfz) gGmbH am Standort Nürnberg angeboten. Es zeigt Unternehmen der regionalen Kunststoffbranche auf, wie sie digitale Inhalte in die Aus- und Weiterbildung integrieren und ihr Ausbildungsmarketing verbessern können. Im Zuge dessen fördert KUKUDI auch die betriebsübergreifende Kooperation und unterstützt die regionalen KMU bei der Umsetzung neuer Ausbildungsinhalte. Gefördert wird das Projekt aus Mitteln des Bundesministeriums für Bildung und Forschung und des Europäischen Sozialfonds.
Weitere Informationen: www.bfz.de/kukudi-kunststoffkmuumbruchdigitalisierung

Ihre Ansprechpartner bei den bfz Nürnberg:

Matthias Gräßel
Telefon: 0911 93197-564
E-Mail: matthias.graessel@bfz.de

Jochen Vogl
Telefon: 0911 93197-850, Mobil: 0160 93959045
E-Mail: jochen.vogl@bfz.de

Gefördert als JOBSTARTER plus-Projekt aus Mitteln des Bundesministeriums für Bildung und Forschung und des Europäischen Sozialfonds.