AGENTUR DER EUROPÄISCHEN UNION
FÜR CYBERSICHERHEIT

KMU-Leitfaden zur Cybersicherheit

12 SCHRITTE

ZUR ABSICHERUNG IHRES UNTERNEHMENS

Die Coronakrise hat die Bedeutung des Internets, und von Computern allgemein, für KMU klar und deutlich aufgezeigt. Um während der Pandemie zu florieren, mussten viele KMU Notfallmaßnahmen zur Aufrechterhaltung des Geschäftsbetriebs einleiten: sie nutzten Cloud-Dienste, verbesserten ihr Internetangebot, aktualisierten ihre Internetseiten und ermöglichten es Mitarbeitern, von zu Hause aus zu arbeiten.

Diese Broschüre enthält Informationen für KMU mit 12 praktischen Schritten zur besseren Absicherung ihrer Systeme und Geschäftstätigkeiten. Sie begleitet den ausführlicheren ENISA-Bericht zu Herausforderungen und Empfehlungen für KMU im Bereich der Cybersicherheit: ***„Cybersecurity for SMES – Challenges and Recommendations"***

1 FÜR EINE GUTE CYBERSICHERHEITS-KULTUR SORGEN

ZUSTÄNDIGKEIT FESTLEGEN

Eine robuste Cybersicherheit ist ein Schlüsselfaktor für den Erfolg. Übertragen Sie die Verantwortung für diese wichtige Aufgabe einer Person in Ihrem Unternehmen, die sich um angemessene Ressourcen kümmert, etwa um Personalzeit, den Einkauf von Software, Dienstleistungen und Hardware für Cybersicherheit, Mitarbeiterschulungen und die Entwicklung wirksamer Konzepte.

MITARBEITER MOTIVIEREN

Motivieren Sie Ihre Mitarbeiter durch wirksame Kommunikation zum Thema Cybersicherheit, unterstützen Sie entsprechende Initiativen, führen Sie geeignete Mitarbeiterschulungen durch und legen Sie in Ihrem Cybersicherheitskonzept eindeutige Regeln für das Personal fest.

CYBERSICHHEITSKONZEPT BEKANNT MACHEN

Legen Sie in Ihrem Cybersicherheitskonzept klare, spezifische Verhaltensregeln für die Mitarbeiter dar, die bei der Nutzung der IT-Strukturen, -Ausrüstung und -Leistungen des Unternehmens einzuhalten sind. Darin sind auch die Folgen für Mitarbeiter, die gegen die Regeln verstoßen, zu beschreiben. Das Konzept muss regelmäßig überprüft und aktualisiert werden.

CYBERSICHERHEITSAUDITS DURCHFÜHREN

Lassen Sie regelmäßig Audits von Personen mit entsprechenden Kenntnissen und Kompetenzen sowie Erfahrung in dem Bereich durchführen. Die externen oder auch betriebseigenen Prüfer sollten unabhängig und nicht in das IT-Tagesgeschäft eingebunden sein.

DATENSCHUTZ BEACHTEN

Nach der EU-Datenschutz-Grundverordnung[1] müssen auch KMU, die personenbezogene Daten von in der EU/im EWR ansässigen Personen verarbeiten oder speichern, für angemessene Sicherheitskontrollen zum Schutz dieser Daten sorgen. Dazu gehört auch, sicherzustellen, dass alle vom Unternehmen beauftragten Dritten angemessene Sicherheitsvorkehrungen treffen.

1 Datenschutz-Grundverordnung: https://ec.europa.eu/info/law/law-topic/data-protection_de

2

GEEIGNETE SCHULUNGEN ANBIETEN

Schulen Sie alle Ihre Mitarbeiter regelmäßig zum Thema Cybersicherheit, damit sie entsprechende Bedrohungen erkennen und damit umgehen können. Die Schulungen sollten speziell auf KMU abgestimmt und realitätsnah sein.

Die in Ihrem Unternehmen für Cybersicherheit zuständigen Personen sollten an speziellen Schulungen teilnehmen, damit sie ihre Aufgaben kompetent erfüllen können.

3

DRITTE EFFEKTIV MANAGEN

Sorgen Sie dafür, dass alle Vertragspartner, insbesondere solche, die Zugang zu sensiblen Daten oder Systemen haben, aktiv gemanagt werden und die vereinbarten Sicherheitsvorgaben erfüllen. In Ihren Vereinbarungen sollte geregelt sein, wie Ihre Vertragspartner die Sicherheitsanforderungen gewährleisten.

4

VORFALL-REAKTIONS-PLAN AUFSTELLEN

Erstellen Sie einen Vorfallreaktionsplan mit klar dokumentierten Leitlinien, Rollen und Zuständigkeiten, um eine zeitnahe, professionelle und angemessene Reaktion auf alle Sicherheitsvorfälle zu gewährleisten. Damit Sie schnell reagieren können, bemühen Sie sich um Tools für die Überwachung und Alarmierung im Fall verdächtigter Aktivitäten oder Sicherheitsverletzungen.

5 SYSTEM-ZUGRIFF ABSICHERN

Bitten Sie alle Mitarbeiter, eine Passphrase aus mindestens drei beliebigen Wörtern zu verwenden, die einprägsam ist und eine hohe Sicherheit bietet. Wird ein gewöhnliches Passwort verwendet, sollte Folgendes beachtet werden:

- Je länger, desto besser; Klein- und Großbuchstaben verwenden sowie möglichst auch Zahlen und Sonderzeichen,
- einfache Passwörter wie „Passwort“ oder Buchstaben- und Zahlenreihen wie „abc“, „123“ usw. vermeiden,
- persönliche Angaben, die im Netz zu finden sind, vermeiden,

Gleich, ob Sie Passphrasen oder Passwörter benutzen:

- Verwenden Sie sie niemals anderswo!
- Teilen Sie sie niemals den Kollegen mit!
- Aktivieren Sie die Multi-Faktor-Authentisierung!
- Nutzen Sie einen speziellen Passwort-Manager!

6 GERÄTE ABSICHERN

Ein wichtiges Element in jedem Cybersicherheitsplan ist der Schutz aller vom Personal verwendeten Geräte, ob Desktop-Computer, Laptops, Tablets oder Mobiltelefone, vor Angriffen.

SOFTWARE-PATCHES UND -UPDATES

Nutzen Sie möglichst eine zentrale Plattform für das Patch-Management.
Sie sollten unbedingt:

- alle Anwendungen regelmäßig aktualisieren,
- wenn möglich, die automatische Aktualisierungsfunktion aktivieren,
- die Hardware und Software ermitteln, die manuell zu aktualisieren sind,
- mobile sowie IdD-Geräte nicht vergessen!

ANTIVIRENSCHUTZ

Auf allen Geräten sollte ein zentral verwalteter Antivirenschutz installiert und stets aktuell gehalten werden, um ständige Wirksamkeit zu gewährleisten. Installieren Sie niemals Raubkopien, da diese Schadprogramme enthalten können.

TOOLS ZUM SCHUTZ VON E-MAILS UND INTERNET

Nutzen Sie Filter für Spam-Mails, E-Mails mit Links zu schädlichen Websites, E-Mails mit schädlichen Dateianhängen, die Viren enthalten können, und Phishing-E-Mails. Installieren Sie niemals Raubkopien, da diese Schadprogramme enthalten können.

VERSCHLÜSSELUNG

Schützen Sie Ihre Daten, indem sie sie verschlüsseln. KMU sollten dafür sorgen, dass die auf mobilen Geräten wie Laptops, Mobiltelefonen und Tablets gespeicherten Daten verschlüsselt sind. Für die Übertragung von Daten über öffentliche Netze wie WLANs in Hotels oder auf Flughäfen sollten entweder ein virtuelles privates Netzwerk (VPN) oder sichere Verbindungen über SSL/TLS-Protokolle benutzt werden. Verwenden Sie auf Ihren eigenen Internetseiten geeignete Verschlüsselungstechniken zum Schutz von Kundendaten, die über das Internet übermittelt werden.

7 IHR NETZWERK ABSICHERN

MOBILE-DEVICE-MANAGEMENT

Viele KMU erlauben Mitarbeitern in Telearbeit die Nutzung ihrer eigenen Laptops, Tablets oder Mobiltelefone. Daraus können sich Sicherheitsbedenken für auf den Geräten befindliche sensible Firmendaten ergeben. Um das Risiko zu begrenzen, können Sie eine Mobile-Device-Management-Lösung (MDM) verwenden, die Folgendes erlaubt:

- Kontrolle, welche Geräte auf Ihre Systeme und Dienstleistungen zugreifen dürfen,
- Sicherstellung, dass das Gerät über ein stets aktuelles Virenschutzprogramm verfügt,
- Festlegung, ob das Gerät verschlüsselt werden soll,
- Prüfung, ob auf dem Gerät die neuesten Software-Patches installiert sind,
- Sicherstellung, dass das Gerät PIN- und/oder passwortgeschützt ist,
- Fernlöschung von Firmendaten, falls das Gerät als gestohlen oder verloren gemeldet wurde oder der Gerätebesitzer das Unternehmen verlässt.

FIREWALLS NUTZEN

Firewalls überwachen den Datenfluss eines Netzwerks und sind damit für KMU ein systemkritisches Tool. Sie sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere als Schutzmauer zwischen Ihrem Netzwerk und dem Internet.

LÖSUNGEN FÜR DEN FERNZUGRIFF

Überprüfen Sie regelmäßig alle Fernzugriff-Tools, um zu gewährleisten, dass sie sicher sind. Achten Sie dabei darauf, dass:

- die Fernzugriff-Software gepatcht und aktualisiert ist,
- kein Fernzugriff von verdächtigten geografischen Orten oder bestimmten IP-Adressen möglich ist,
- der Fernzugriff durch Mitarbeiter auf die für ihre Arbeit nötigen Systeme und Computer beschränkt ist,
- sichere Fernzugriff-Passwörter verwendet werden und, wenn möglich, die Multi-Faktor-Authentisierung aktiviert ist,
- die Überwachungs- und Alarmfunktion aktiviert ist, um vor mutmaßlichen Angriffen und verdächtigen Aktivitäten zu warnen.

8 PHYSISCHE SICHERHEIT VERBESSERN

Alle Geräte, auf denen sich wichtige Informationen befinden, sollten stets angemessen unter Kontrolle sein. Ein Firmenlaptop oder -mobiltelefon beispielsweise sollte nie unbeaufsichtigt auf dem Rücksitz eines Autos liegen. Wenn ein Mitarbeiter seinen Computer verlässt, sollte er ihn jedes Mal sperren. Sie können auf den für Firmenzwecke benutzten Geräten die automatische Sperrung einstellen. Sensible Ausdrucke sollten ebenfalls nicht unbeaufsichtigt herumliegen und bei Nichtverwendung weggeschlossen werden.

9 BACKUPS DURCH-FÜHREN

Führen Sie Datensicherungen durch, damit Sie wichtige Daten wiederherstellen können, etwa im Fall von Angriffen mit Erpressungssoftware. Beachten Sie dabei folgende Regeln:

- Die Backups finden regelmäßig und möglichst automatisch statt.
- Sie werden von der Arbeitsumgebung getrennt aufbewahrt.
- Sie sind verschlüsselt, vor allem wenn die Daten an einen anderen Ort verbracht werden.
- Die reguläre Wiederherstellung der Daten wird getestet. Idealerweise sollten regelmäßige Tests zur kompletten Wiederherstellung von Anfang bis Ende durchgeführt werden.

10

DIE CLOUD NUTZEN

Cloudbasierte Lösungen bieten viele Vorteile, bergen aber auch bestimmte Gefahren, die Sie kennen sollten, bevor Sie sich an einen Cloud-Anbieter wenden. Die ENISA hat hierzu den KMU-Leitfaden zu Cloudsicherheit („*Cloud Security Guide for SMEs*“[2]) erstellt, den Sie bei einer Datenmigration in die Cloud zu Rate ziehen sollten.

Stellen Sie bei der Auswahl eines Cloud-Anbieters sicher, dass bei der Speicherung von – insbesondere personenbezogenen – Daten außerhalb der EU/des EWR nicht gegen Gesetze oder Vorschriften verstoßen wird. Die Datenschutz-Grundverordnung der EU verlangt beispielsweise, dass personenbezogene Daten von in der EU oder dem EWR ansässigen Personen nur unter bestimmten Umständen außerhalb der EU/des EWR gespeichert oder übermittelt werden dürfen.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 IHRE INTERNET-PRÄSENZEN ABSICHERN

Stellen Sie sicher, dass Ihre Internetseiten sicher konfiguriert sind und gepflegt werden und dass alle personenbezogenen Daten und Finanzangaben wie etwa Kreditkartendetails angemessen geschützt sind. Dazu gehört, die Internetseiten regelmäßig auf potenzielle Sicherheitslücken hin zu testen und regelmäßig zu überprüfen, ob sie ordnungsgemäß gepflegt und aktualisiert werden.

12 INFORMATIONEN GEWINNEN UND WEITERGEBEN

Ein wirksames Instrument im Kampf gegen Cyberkriminalität ist der Informationsaustausch. Die Weitergabe von Informationen über Kriminalität im Internet ist wichtig, damit KMU verstehen, welchen Risiken sie ausgesetzt sind. Unternehmen, die von Gleichgesinnten hören, welche Probleme aufgetreten sind und wie diese gemeistert wurden, sind eher geneigt, ihre Systeme abzusichern, als solche, die nur in Branchenstudien oder Erhebungen zur Cybersicherheit darüber lesen.

AGENTUR DER EUROPÄISCHEN UNION
FÜR CYBERSICHERHEIT

ÜBER ENISA

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einem hohen gemeinsamen Maß an Cybersicherheit in ganz Europa beizutragen. Sie wurde im Jahr 2004 gegründet und durch den Rechtsakt zur Cybersicherheit in ihrem Mandat weiter gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, kooperiert mit den Mitgliedstaaten und Organen und Einrichtungen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Kapazitätsaufbau und Sensibilisierung arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und nicht zuletzt ein sicheres digitales Umfeld für die Gesellschaft und die Bürgerinnen und Bürger Europas zu gewährleisten.
Weitere Informationen finden Sie auf www.enisa.europa.eu.

ENISA
Agentur der Europäischen Union für Cybersicherheit

Büro in Athen
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki, Griechenland

Büro in Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Griechenland

enisa.europa.eu