Checkliste für Ihre Cyber-Sicherheit

Es gibt einige effiziente Maßnahmen, um die Cyber-Sicherheit in Anbetracht der aktuellen Situation kurzfristig zu erhöhen.

Anhand der folgenden Checkliste können Sie überprüfen, welche Cyber-Sicherheitsmaßnahmen Sie sinnvoller Weise umsetzen können, um Ihr Unternehmen jetzt besser zu schützen.

Hinweise zur Durchführung von Cyber-Sicherheitsmaßnahmen, um das Risiko von Angriffen zu reduzieren.

1.1 Maßnahmen zur Vermeidung von Angriffen

- Geschäftskritische Daten sollten möglichst nicht auf Endgeräten gespeichert werden: Haben Sie alle Endgeräte überprüfen lassen, ob darauf geschäftskritische Daten vorhanden sind, die nicht mehr benötigt werden?

  ☐ Ja ☐ Nein

- Updates erhöhen das Schutzniveau: Haben Sie veranlasst, dass auf allen relevanten IT-Systemen die aktuellen Updates eingespielt worden sind?

  ☐ Ja ☐ Nein

- Über Apps können Angriffe erfolgen: Haben Sie festgelegt, dass nur autorisierte Apps ausgeführt werden dürfen?

  ☐ Ja ☐ Nein

- Supply Chain-Angriffe stellen momentan ein Problem dar: Haben Sie eine Richtlinie erstellt zur sicheren Integration von Codes und externen Diensten?

  ☐ Ja ☐ Nein

- Ungenutzte Software bietet eine Angriffsfläche: Haben Sie Ihre IT-Systeme dahingehend überprüfen und unnötige Software, beziehungsweise Programme und Apps, entfernen lassen?

  ☐ Ja ☐ Nein

- Zugriffsrechte ermöglichen Angriffe: Haben Sie die Rechtevergabe kritisch auf ihre tatsächliche Notwendigkeit hin überprüfen und entsprechend einschränken lassen?

  ☐ Ja ☐ Nein

- Jeder (nicht notwendige) offene Port ist eine potenzielle Schwachstelle: Haben Sie die Kommunikationsmöglichkeiten durch Einstellungen in Ihren Routern und Firewall-Systemen reduzieren lassen?

  ☐ Ja ☐ Nein

- Know-how hilft Angriffe zu vermeiden: Haben Sie die notwendigen Schritte eingeleitet, um Ihre Administratoren regelmäßig zu schulen und ihnen das relevante Wissen bezüglich aktuelle Angriffsszenarien zu vermitteln und dafür zu sensibilisieren?

  ☐ Ja ☐ Nein

- Know-how hilft Angriffe zu vermeiden: Sind regelmäßige Schulungen – abgestuft gemäß der Kritikalität – auch für die Mitarbeitenden im Homeoffice eingeplant?

  ☐ Ja ☐ Nein

1.2 Maßnahmen zum Entgegenwirken von Angriffen

- Datei-, Festplatten-, E-Mail-Verschlüsselung/VPN-Systeme: Haben Sie veranlasst, dass Ihre geschäftskritischen und personenbezogenen Daten ausreichend durch Verschlüsselung geschützt sind?

  ☐ Ja ☐ Nein

- Verantwortlichkeit: Wird Ihre Anti-Malware-Lösung zentral administriert?

  ☐ Ja ☐ Nein

- Aktualisierung: Ist sichergestellt, dass die Malwaresignaturen automatisiert und zeitnah bereitgestellt werden?

  ☐ Ja ☐ Nein

- Umfassender Schutz: Haben Sie überprüfen lassen, ob Updates der Anti-Malware-Lösung erfolgreich auf allen Clients ausgerollt wurden?

  ☐ Ja ☐ Nein

Hinweise zur Durchführung von Cyber-Sicherheitsmaßnahmen, um mit den verbliebenden Risiken umgehen zu können.

2.1 Maßnahmen zum Erkennen von Angriffen

- Eine frühzeitige Angriffserkennung ist essenziell: Haben Sie ein Intrusion Detection (IDS)- / Intrusion Prevention (IPS)-System im Einsatz?

  ☐ *Ja* ☐ Nein

- Ihre Angestellten müssen wissen, wie sie sich verhalten sollen: Haben Sie Ihre Mitarbeitenden dahingehend geschult, dass sie potenzielle Angriffe so schnell wie möglich melden?

  ☐ Ja ☐ Nein

- Ihre Angestellten müssen wissen, an wen sie sich wenden sollen: Haben Sie eine verantwortliche Person benannt/ eine Meldestelle etabliert, damit bei einer Meldung / im Angriffsfall umgehend die notwendigen Schritte eingeleitet werden können?

  ☐ Ja ☐ Nein

2.2 Maßnahmen als Reaktion auf Angriffe

- Im Falle eines Angriffs müssen alle Firewall und E-Mail-Server-Regeln eingeschränkt werden: Haben Sie ein Konzept, in dem die relevanten Prozesse ihres Unternehmens beschrieben sowie die notwendigen Regeln definiert sind?

  ☐ Ja ☐ Nein

- Im Angriffsfall benötigen Sie genügend qualifizierte Mitarbeitende vor Ort: Haben Sie einen entsprechenden Notfall-/Einsatzplan, um sicherzustellen, dass die Verantwortlichkeiten und Zuständigkeiten Ihrer Mitarbeitenden genau definiert sind und zeitnah reagiert werden kann?

  ☐ Ja ☐ Nein

Checkliste Cyber-Sicherheit – Auswertung

Die Checkliste soll dazu dienen, Sie mit kurzfristigen Maßnahmen zur Reduzierung des Risikos von Angriffen vertraut zu machen sowie für den Umgang mit den verbleibenden Risiken zu sensibilisieren und nicht zuletzt Ihnen Anhaltspunkte aufzeigen, wo eventuell noch Lücken bestehen.

Wenn Sie alle Fragen mit „Ja“ beantwortet haben, sind Sie auf dem richtigen Weg. Die mit „Nein“ beantworteten Fragen, zeigen Ihnen auf, in welchen Bereichen noch Handlungsbedarf besteht. Wenn Sie bezüglich des Handlungsbedarfs weitere Informationen wünschen, stellen wir Ihnen diese gerne zur Verfügung: Anfrage mit Stichwort „Checkliste“ bitte an info@hego-it.com senden.

Für den Fall, dass Sie weniger als 6 Fragen mit „Ja“ beantworten konnten, sollten Sie – aufgrund der aktuellen Situation – aktiv werden. Wir unterstützen Sie dabei gerne – vereinbaren Sie einfach unverbindlich einen ersten Termin zum Kennenlernen.