Selbstassessment für die Unternehmensleitung

Wie gut ist Ihr Unternehmen vor Angriffen aus dem Cyberspace geschützt und darauf vorbereitet?

Dieses Selbstassessment soll der Unternehmensleitung helfen, sich mit den wichtigsten Fragen für einen minimalen Cybersecurity-Schutz auseinanderzusetzen. Je mehr «Ja» Sie ankreuzen, desto besser. Ein «Weiss nicht» oder ein «Nein» bedeutet, dass Sie entsprechende Abklärungen vornehmen sollten. Dabei gilt: Massnahmen zum Schutz vor Cyberangriffen lassen sich nicht an Mitarbeitende delegieren, sondern müssen von der Geschäftsleitung angegangen und koordiniert werden.

Weitere Informationen finden Sie auf www.cybersecurity-check.ch und www.melani.admin.ch

	Ja	Nein	Weiss nicht
Aufgaben, Kompetenzen, Verantwortlichkeiten			
Ist in Ihrem Betrieb bestimmt, wer für Cybersecurity verantwortlich ist?	○	○	○
Hat die verantwortliche Person das notwendige Wissen und die Fähigkeiten, um mit Cybersecurity umzugehen und bildet sie sich regelmässig weiter?	○	○	○
Hat die verantwortliche Person die notwendige hierarchische Stellung und entsprechende Kompetenzen, um Cybersecurity-Massnahmen umzusetzen?	○	○	○
Gibt es Richtlinien für den sicheren Umgang mit IT-Geräten und mit Daten?	○	○	○
Werden diese Richtlinien und Cybersecurity-Massnahmen konsequent und systematisch umgesetzt und regelmässig überprüft?	○	○	○
Sensibilisierung von Mitarbeitenden			
Existieren für Ihre Mitarbeitenden betriebliche Richtlinien zum sicheren Umgang mit E-Mails, digitalen Daten und Internet?	○	○	○
Kennen und verstehen die Mitarbeitenden diese Richtlinien?	○	○	○
Setzen die Mitarbeitenden die Richtlinien konsequent und korrekt um?	○	○	○
Werden die Mitarbeitenden regelmässig bezüglich Cybersecurity, zum Beispiel korrekter Umgang mit E-Mails, geschult bzw. sensibilisiert?	○	○	○
Datenschutz-Richtlinien			
Sind Daten auf Ihren Systemen (Datenablagen und -speicher, Endgeräte und Server) verschlüsselt?	○	○	○
Sind Sie sich der gesetzlichen Vorschriften bezüglich Datenspeicherung und -verarbeitung bewusst?	○	○	○
Kennen Sie Ihre Pflichten im Zusammenhang mit den Vorschriften bezüglich personenbezogener Daten?	○	○	○
Werden die aktuell geltenden Vorschriften zum Datenschutz in Ihrem Betrieb konsequent und korrekt umgesetzt?	○	○	○
Ist in Ihrem Betrieb der physische Zugang zur Rechner-, Server- und Netzwerkinfrastruktur vor dem Zugriff von Dritten zweckmässig geschützt?	○	○	○
Passwort-Richtlinien und Benutzeradministration			
Gibt es in Ihrem Betrieb Richtlinien zur Verwendung von Passwörtern?	○	○	○
Gibt es Richtlinien, die definieren, welche Mitarbeitenden auf welche Daten Zugriff haben?	○	○	○
Werden diese Richtlinien konsequent und korrekt umgesetzt?	○	○	○

	Ja	Nein	Weiss nicht
Aktueller Schutz vor schädlicher Software			
Sind Ihre Geräte gegen bösartige Software geschützt (Antivirus-Programm)?	○	○	○
Konfigurierte und aktualisierte Firewall			
Sind Ihr Unternehmensnetzwerk und Ihre IT-Systeme durch eine Firewall geschützt?	○	○	○
Wurden spezielle Firewall-Regeln definiert (zum Beispiel geografische Einschränkung)?	○	○	○
Wird Ihre Firewall regelmässig aktualisiert?	○	○	○
Netzwerksegmentierung			
Sind die einzelnen Bereiche Ihres Unternehmens, zum Beispiel Personal, Buchhaltung und Produktion, getrennt?	○	○	○
Verwenden Sie einen separaten Computer oder ein separates System nur für E-Banking?	○	○	○
Fernzugriff			
Ist in Ihrem Betrieb der externe Zugang zur Rechner-, Server- und Netzwerkinfrastruktur geschützt (VPN, Zwei-Faktor-Authentifizierung)?	○	○	○
Mit dem Internet verbundene Geräte und Systeme aktuell halten (zum Beispiel Arbeitsplatzsysteme, Produktionsanlagen, Gebäudeleitsysteme)			
Nutzen Sie die Möglichkeit der automatischen Softwareaktualisierung?	○	○	○
Wird bei Geräten und Systemen, deren Software nicht automatisch aktualisiert wird, diese regelmässig auf den neusten Stand gebracht, beispielsweise durch den Hersteller?	○	○	○
Werden die im Firmenumfeld verwendeten Mobilgeräte regelmässig aktualisiert?	○	○	○
Ist Ihr Content Management für Ihren Webauftritt auf dem neuesten Stand?	○	○	○
Geschütztes und verschlüsseltes WLAN-Netzwerk			
Ist Ihr WLAN verschlüsselt und geschützt?	○	○	○
Gibt es je ein separates WLAN für Mitarbeitende und Gäste?	○	○	○
Back-up			
Wenden Sie einen Daten-Back-up-Prozess an?	○	○	○
Überprüfen Sie regelmässig die Funktionsfähigkeit und Lesbarkeit des Back-ups?	○	○	○
Wird das Back-up getrennt (offline) und ausser Haus (offsite) abgelegt?	○	○	○
Mindestvorkehrung für die Notfallbewältigung			
Sind die Sofortmassnahmen im Falle eines IT-Vorfalls definiert?	○	○	○
Ist die verantwortliche Person sowie die Ansprechperson im Falle eines IT-Vorfalls (zum Beispiel Fehlfunktion, Angriff o.Ä.) definiert und verfügbar?	○	○	○
Outsourcing			
Falls Sie IT-Services ausgelagert haben: Sind die oben genannten Punkte dieses Assessments im Vertrag mit dem Dienstleistungsunternehmen abgedeckt?	○	○	○

Basierend auf den Cybersecurity-Schnelltests für KMU von ICTswitzerland und weiteren Partnern, www.cybersecurity-check.ch.
In Zusammenarbeit mit der Kantonspolizei Bern und MELANI.