

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

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

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