CYBERSECURITY-SCHNELLTEST FÜR KMU

Wie gut ist Ihr Unternehmen vor Angriffen aus dem Cyberspace geschützt und darauf vorbereitet? Testen Sie jetzt, ob Sie die Minimalstandards für KMU erfüllen.

Die Risiken von Cyberangriffen werden oft stark unterschätzt. Das hat eine 2017 durchgeführte Befragung bei Geschäftsführerinnen und -führern von KMU in der Schweiz gezeigt [1]. Die Mehrheit der KMU fühlen sich gut geschützt, obwohl häufig zu wenig gegen die Bedrohungen unternommen wird.

Der vorliegende Fragebogen ermöglicht Ihrem Unternehmen eine Standortbestimmung und zeigt Ihnen auf, ob Sie die wichtigsten technischen, organisatorischen und mitarbeiterbezogenen Massnahmen für einen minimalen Cybersecurity-Schutz umsetzen.

Das Ausfüllen dauert nur wenige Minuten. Sollten Sie eine oder mehrere Fragen mit «Nein» oder «Weiss nicht» beantworten, finden Sie unter www.cybersecurity-check.ch zusätzliche Informationen, speziell für KMU.
Wir empfehlen Ihnen dringend, sich mit diesem wichtigen Thema gebührend auseinanderzusetzen.

[1] https://ictswitzerland.ch/publikationen/studien/cyberrisiken-in-schweizer-kmus/

	ja	nein	weiss nicht
1. 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?	☐	☐	☐
2. Sensibilisierung von Mitarbeitenden, Kunden, Lieferanten und Dienstleistern			
Existieren für Ihre Mitarbeitenden betriebliche Richtlinien zum sicheren Umgang mit E-Mail, 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, z.B. korrekter Umgang mit E-Mail, geschult bzw. sensibilisiert?	☐	☐	☐
Tauscht sich Ihr Unternehmen mit Kundinnen und Kunden sowie Lieferanten zur Cybersecurity aus? (auch diese sollten den Schnelltest machen).	☐	☐	☐
3. 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?	☐	☐	☐

	ja	nein	weiss nicht
4. Passwort-Richtlinien und Benutzeradministration			
Gibt es in Ihrem Betrieb Richtlinien zur Verwendung von Passwörtern?	☐	☐	☐
Gibt es Richtlinien, nach denen Administrationsrechte systematisch vergeben werden?	☐	☐	☐
Gibt es Richtlinien, die definieren, welche Mitarbeitenden auf welche Daten Zugriff haben?	☐	☐	☐
Werden diese Richtlinien konsequent und korrekt umgesetzt?	☐	☐	☐
5. Aktueller Schutz vor schädlicher Software			
Sind Ihre Geräte gegen bösartige Software geschützt (z.B. Antivirus-Programm, Spam-Filter)?	☐	☐	☐
6. Konfigurierte und aktualisierte Firewall			
Sind Ihr Unternehmensnetzwerk und Ihre IT-Systeme durch eine Firewall geschützt?	☐	☐	☐
Wird Ihre Firewall regelmässig aktualisiert?	☐	☐	☐
7. Mit dem Internet verbundene Geräte und Systeme aktuell halten (z.B. Arbeitsplatzsysteme, Produktionsanlagen, Gebäudeleitsysteme, usw.)			
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 (z.B. durch den Hersteller)?	☐	☐	☐
Werden die im Firmenumfeld verwendeten Mobilgeräte regelmässig aktualisiert?	☐	☐	☐
8. Geschütztes und verschlüsseltes WLAN-Netzwerk			
Ist Ihr WLAN verschlüsselt und geschützt?	☐	☐	☐
Gibt es ein separates (getrenntes) WLAN für Mitarbeitende und Gäste?	☐	☐	☐

	ja	nein	weiss nicht
9. Verschlüsselung von (Daten-)Übermittlung (z.B. VPN)			
Verwenden Sie generell und durchgehend gesicherte und verschlüsselte Kommunikationsverbindungen im Internet?	☐	☐	☐
10. Backup			
Wenden Sie einen Daten-Backup-Prozess an?	☐	☐	☐
Überprüfen Sie regelmässig die Funktionsfähigkeit und Lesbarkeit des Backups?	☐	☐	☐
Wird das Backup physisch getrennt (offline) abgelegt?	☐	☐	☐
11. Mindestvorkehrung für die Notfallbewältigung			
Sind die Sofortmassnahmen im Falle eines IT-Vorfalls definiert?	☐	☐	☐
Ist der bzw. die Verantwortliche sowie die Ansprechperson im Falle eines IT-Vorfalls (z.B. Fehlfunktion, Angriff o.ä.) definiert und verfügbar?	☐	☐	☐
12. Outsourcing			
Falls Sie IT-Services ausgelagert haben: Sind die Punkte 1-11 dieses Fragebogens im Vertrag mit dem Servicepartner abgedeckt?	☐	☐	☐

Sie haben sich mit den wichtigsten Fragen für einen minimalen Cybersecurity-Schutz auseinandergesetzt. Eine Zusammenstellung mit weiterführenden Informationen – speziell für KMU – finden Sie auf www.cybersecurity-check.ch.

Impressum

Autoren:

Umberto Annino (ISSS) | Norbert Bollow (SNV) |Maya Bundt (SVV) | Daniel Caduff (BWL) | Lucius Dürr (SQS) | Xaver Edelmann (SQS) | Andreas Kaelin (ICTswitzerland) | Marcel Knecht (SNV) | Arié Malz (EFD) | Felix Müller (SQS) | Gunthard Niederbäumer (SVV) | Reinhard Niederer (Druckerei AG Suhr) | Peter Reber (SQS) | Daniel Rudin (ISB – MELANI) | Ronald Trap (SNV)

Redaktion:

Annalena Kassner (ICTswitzerland) | Lena Schneider (ICTswitzerland) | Adrian Sulzer (SATW) | Nicole Wettstein (SATW)