Cyberdelikte verhindern

Wegleitung für kleine und mittlere Unternehmen

Wissen Sie, wie gut Ihr Unternehmen geschützt ist?

Prüfen Sie es mithilfe der Checkliste am Ende dieser Broschüre!

Inhaltsverzeichnis

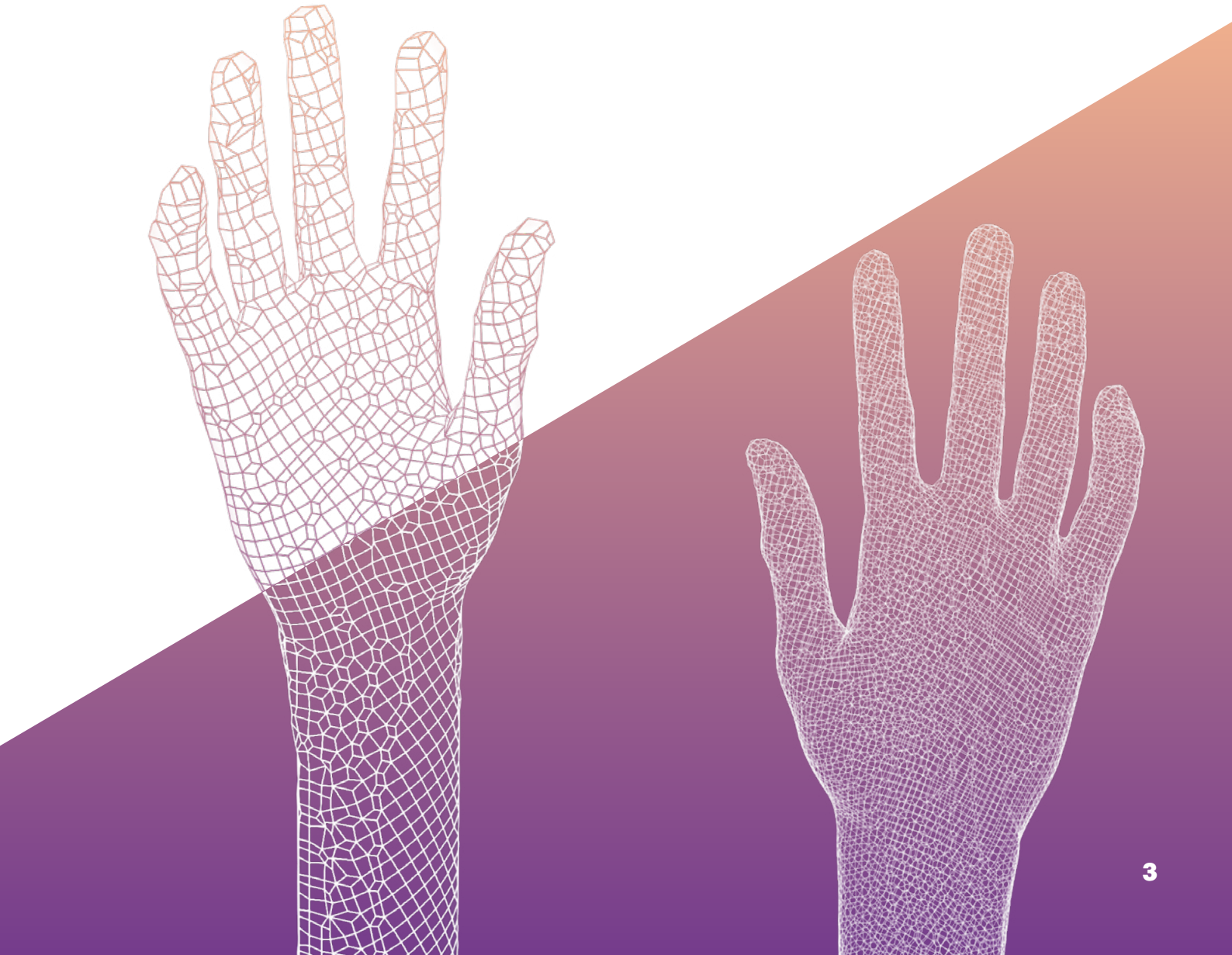
1_Cybersicherheit in Unternehmen als existenzieller Aspekt

Die Digitalisierung eröffnet der Wirtschaft neue Wachstumschancen und Beschäftigungsmöglichkeiten. Zugleich erfordert sie neue Prozesse und führt zu einer grösseren Abhängigkeit von funktionierender Informations- und Kommunikationstechnik (IKT). Diese Abhängigkeiten nutzen auch Kriminelle aus.

Um sich Zugang zu Netzwerken zu verschaffen, Daten zu stehlen oder gesamte Systeme lahmzulegen verwendet die Täterschaft immer ausgefeiltere Methoden. Vom kleinen Handwerksbetrieb bis zur Grossfirma: Ein Cyberangriff kann für Unternehmen zur existenziellen Bedrohung werden.

Mit dem vorliegenden Informationsmaterial gibt die Polizei grundlegende Empfehlungen für Kadermitglieder von kleinen und mittelgrossen Unternehmen zum Schutz vor Cyberkriminalität.

Die Inhalte stützen sich unter anderem auf Erfahrungen aus der polizeilichen Ermittlungstätigkeit.
Die Wegleitung zeigt ausserdem auf, was nach einem Angriff zu tun ist und weshalb sich der Gang zur Polizei lohnt.



2_So gehen Kriminelle vor

Angriffe beginnen in der Regel damit, dass sich Kriminelle über das Unternehmen informieren. Gestützt auf Informationen auf der Firmen-Website oder in den sozialen Medien werden Schwachstellen im Unternehmensumfeld ausgemacht, mögliche Einfallstore im Unternehmensnetzwerk identifiziert und ein passendes Angriffsszenario erarbeitet.

2.1 Typische Einfallstore

Manipulation

Kriminelle nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Mitarbeitenden aus, um ihnen sicherheitsrelevante Informationen zu entlocken oder um Zugang zu Unternehmensnetzwerken zu erlangen («Social Engineering»). Durch die Kontaktaufnahme per E-Mail («Phishing») oder Telefon versucht die Täterschaft, Personen zur Herausgabe von sensiblen Daten zu bewegen. Mittels Versand von verseuchten Anhängen in betrügerischen Nachrichten oder Links auf infizierte Webseiten gelingt es Kriminellen, Schadsoftware auf Geräte einzuschleusen und so Zugang zu den Netzwerken eines Unternehmens zu erhalten.

Eine besonders tückische und verbreitete Form der Manipulation ist das sogenannte «Spear Phishing». Den gezielt ausgewählten Opfern wird vorgegaukelt, mit vertrauten Personen, Organisationen oder Unternehmen zu kommunizieren. Weil die Quelle der Nachrichten scheinbar bekannt ist und Informationen plausibel erscheinen, kommt es vor, dass selbst aufmerksame Personen die Manipulation nicht erkennen.

Fernzugriff (Remote Access)

Remote Access dient dazu, von ausserhalb auf einen Computer oder ein Netzwerk zuzugreifen, beispielsweise für Arbeiten im Homeoffice oder zwecks Fernwartung durch Supportmitarbeitende. Auch Kriminelle nutzen diesen Fernzugang, um auf Unternehmensnetze zu gelangen. Dies insbesondere dann, wenn der Fernzugriff ungenügend geschützt ist.

Schwachstellen in Anwendungen

Das Ausnutzen von Schwachstellen in Anwendungen ist ebenfalls eine häufige Vorgehensweise bei Cyberangriffen. Es kann sich dabei um Software-Schwachstellen, Design-Schwachstellen oder um schlecht konfigurierte Schutzparameter, beispielsweise schwache Passwörter, handeln.

Weitere Informationen zu aktuellen Cyberbedrohungen finden Sie unter

www.ncsc.admin.ch

2.2 Mögliche Angriffsszenarien

Verschlüsselung, Diebstahl oder Beschädigung von Daten

Daten werden bei einem Angriff entweder verschlüsselt und nur gegen ein Lösegeld wieder freigegeben («Ransomware»), gestohlen und gewinnbringend, beispielsweise im Darknet weiterverkauft («Datenabfluss»), oder die Daten werden verwendet, um betroffene Drittunternehmen zu erpressen. Der nicht autorisierte Zugang zu einem Datenverarbeitungssystem kann auch die Zerstörung von Daten bezwecken, etwa mit dem Ziel, einen Vorteil gegenüber der Konkurrenz zu erlangen oder ein laufendes Geschäft zu blockieren.
Angriffe können dabei sowohl von aussen wie auch von innen erfolgen: Mitarbeitende können ebenfalls vertrauliche Firmendaten manipulieren, vernichten oder an Unberechtigte weitergeben.

CEO-Betrug

Es handelt sich in der Regel um einen massgeschneiderten Angriff mit Informationen, die im Vorfeld über das Unternehmen gesammelt wurden. Der Betrug erfolgt häufig mittels gefälschter E-Mail der Unternehmensleitung oder von Vereinsvorsitzenden an die Finanzabteilung beziehungsweise an Personen mit Kassier-Funktion. Durch eine glaubwürdige Geschichte soll die angeschriebene Person dazu bewegt werden, angeblich dringende Zahlungen auszulösen.

Rechnungsmanipulationsbetrug

Die Täterschaft verschickt bereits versendete Rechnungen mit geänderter IBAN-Nummer ein weiteres Mal oder weist die Opfer an, für zukünftige Zahlungen ein anderes Empfängerkonto zu benutzen. Dabei wird auf eine bestehende E-Mail-Kommunikation Bezug genommen, die eine Zahlungsanweisung oder eine Rechnung enthält. Das heisst, Kriminelle hatten sich im Vorfeld entweder auf das E-Mail-Konto der absendenden Person oder auf jenes der empfangenden Person Zugriff verschafft.

Überlastattacke

Bei einem «Distributed Denial of Services-Angriff» (DDoS) werden Systeme oder Netzwerke eines Unternehmens komplett überlastet, so dass diese vorübergehend nicht erreichbar sind. Der Angriff wird so lange aufrechterhalten, bis ein Lösegeld gezahlt wird. Unternehmen, die beispielsweise einen Webshop haben, müssen bei einem DDoS-Angriff mit erheblichen Gewinneinbussen oder entgangenen Aufträgen rechnen. Bei dieser Angriffsart ist vorgängig kein Zugang zum Netzwerk eines Opfers nötig.

Physischer Angriff

Auch die physische IKT-Infrastruktur eines Unternehmens kann angegriffen werden, zum Beispiel indem Datenleitungen sabotiert oder elektronische Geräte und Datenträger manipuliert werden.

3_So schützen Sie Ihr Unternehmen

Schutz vor Cyberkriminalität sollte Teil eines ganzheitlichen und umfassenden Sicherheitskonzepts sein. Dieses ist sowohl technologisch wie auch organisatorisch ausgerichtet.

3.1 Klären Sie die Verantwortlichkeiten

Definieren Sie klare Rollen und Verantwortlichkeiten im Bereich der Cybersicherheit.
Falls Sie Ihre IKT an Externe ausgelagert haben, regeln Sie die Zuständigkeiten vertraglich. Die Verantwortung für die Cybersicherheit Ihres Unternehmens bleibt jedoch weiterhin bei Ihnen.
Auch die Mitarbeitenden müssen wissen, an wen sie sich wenden sollen, wenn sie Fragen zur IKT-Sicherheit haben, zum Beispiel bei Erhalt eines verdächtigen E-Mails oder wer bei einem Vorfall zu informieren ist.

3.2 Regeln Sie den Zugriff auf Systeme

Berechtigungen und Regeln

Definieren Sie, welche Daten in Ihrem Unternehmen als besonders schützenswert gelten. Erstellen Sie für diese Elemente ein spezifisches Schutzkonzept. Dazu gehört, die Nutzungsrechte und Zugriffsberechtigungen auf Daten und Systeme zu definieren und die Verwendung privater Geräte, welche für geschäftliche Tätigkeiten genutzt werden, zu regeln.

Mitarbeitende dürfen nicht über Administratorenrechte verfügen. Es gilt, Mitarbeitenden nur diejenigen Rechte zu gewähren, welche sie für die Ausführung der ihnen zugewiesenen Arbeiten benötigen (Need-to-know-Prinzip). Schränken Sie die Systemrechte so ein, dass Mitarbeitende nicht eigenständig Installationen oder Updates von Software vornehmen können.
Administratoren müssen mit einem für diese Tätigkeit konfigurierten und vom Mitarbeitenden-Account getrennten spezifischen Admin-Account arbeiten.

Definieren Sie verbindliche Passwortregeln für Passwörter hoher Komplexität und Länge und setzen Sie diese auch gegenüber Mitarbeitenden konsequent durch. Richten Sie für den Zugang in Ihr Unternehmensnetzwerk eine Multifaktor-Authentifizierung ein. Dies gilt insbesondere für Administratoren oder andere privilegierte Konten.

Überlegen Sie genau, welche Informationen – auch scheinbar harmlose – Sie auf der Unternehmenswebsite oder in sozialen Medien offenlegen, denn diese werden von Kriminellen gesammelt und können für gezielte Angriffe verwendet werden.

So erstellen Sie ein sicheres Passwort

Ein gutes Passwort:

Besteht aus mindestens zwölf Zeichen, enthält Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Kommt in keinem Wörterbuch vor, ist zufällig generiert und enthält keine persönlichen Informationen.

Wird nur für eine einzige Anwendung verwendet. Sollte ein Passwort geknackt werden, ist so nur ein Login betroffen.
Ein Passwortmanager hilft Ihnen, die unterschiedlichen Zugangsdaten für verschiedene Anwendungen zu verwalten.

Wird mit einer Zwei-Faktor-Authentifizierung ergänzt.

Befolgen Sie oben genannte Regeln. Eine zyklische Passwortänderung ist unnötig. Passwörter müssen gewechselt werden, wenn sie Dritten bekannt sein könnten oder wenn Mitarbeitende nicht mehr in Ihrem Unternehmen tätig sind.

Geschützte und dokumentierte IKT-Infrastruktur

Netzwerkinfrastruktur, Büro- und mobile Geräte sowie Spezialausrüstungen müssen gegen unbefugten Zugriff, Verlust, Diebstahl oder Zerstörung geschützt werden. Binden Sie Sicherheitsüberlegungen bereits in den Beschaffungsprozess der IKT-Infrastruktur ein. Nicht nur die Anforderungen bei der Inbetriebnahme, sondern für den gesamten Lebenszyklus eines Systems inklusive Wartung und Entsorgung sind zu berücksichtigen. Informieren Sie sich beispielsweise, wie lange Sicherheits-Updates für Ihre Geräte zur Verfügung gestellt werden. Dokumentieren Sie Ihr gesamtes Netzwerk. Die Daten, Personen, Geräte, Systeme und Anlagen Ihres Unternehmens sollten identifiziert, katalogisiert und in Bezug auf ihre Kritikalität bewertet werden. Nur so wissen Sie, was Sie schützen müssen. Auch wenn Sie Ihre IKT ausgelagert haben, müssen Sie den Überblick behalten: Sie tragen die Verantwortung.

Sicheres E-Banking

Klären Sie sämtliche Prozesse, welche den Zahlungsverkehr betreffen. Setzen Sie die Einhaltung dieser Prozesse konsequent durch; beispielweise Vier-Augen-Prinzip, Kollektivunterschrift, Rückfragen über einen zweiten Kanal, insbesondere bei Kontoänderungen. Verwenden Sie für Zahlungen nach Möglichkeit einen separaten Computer, auf welchem Sie nicht im Internet surfen oder E-Mails empfangen, den Sie aber dennoch regelmässig updaten. Alternativ können Sie Online-Zahlungen in einem von den restlichen Anwendungen abgegrenzten Bereich («Sandboxing») oder in einem dedizierten, besonders geschützten virtualisierten System tätigen.
Sprechen Sie mit Ihrer Bank über diese und weitere Sicherheitsmassnahmen.

Verschlüsselte Kommunikation

Vertrauliche Informationen müssen verschlüsselt gespeichert (dies gilt auch für die Cloud) und übermittelt oder per Briefpost an externe Stellen gesendet werden. Der Zugriff auf Daten muss - im speziellen wenn Mitarbeitende von extern auf das Firmennetzwerk zugreifen - über einen sicheren Kanal wie zum Beispiel ein VPN erfolgen. Kommunizieren Sie auch achtsam mit Ihrer Kundschaft sowie mit Ihren Partnerunternehmen. Signieren Sie in einem ersten Schritt ausgehende E-Mails. Damit garantieren Sie deren Integrität und Herkunft. Durch die digitale E-Mail-Signatur haben Kunden zudem die Möglichkeit, Antwort-E-Mails an Sie zu verschlüsseln. Alternativ können Sie Verschlüsselungszertifikate für Ihre Nachrichten verwenden.

Die Nutzung von externen und öffentlichen Access Points (Hotspots) muss speziell geregelt werden, da solche generell nicht verschlüsselt sind und somit als unsicher gelten.

Cloud

Bei Clouddiensten gilt das Gleiche wie bei jeder Geschäftspartnerschaft: Achten Sie bei der Auswahl des Cloud-Anbieters auf die Seriosität des Unternehmens (Zertifikate, Datenlokation, Berichte, Tests etc.).
Bauen Sie eine vertrauenswürdige Beziehung auf und klären Sie Ihre Bedürfnisse und die jeweiligen Verantwortlichkeiten. Lesen Sie vor der Nutzung eines Clouddienstes die Allgemeinen Geschäftsbedingungen des Anbieters und achten Sie auf die Datenschutzbestimmungen.

Überlegen Sie genau, welche Daten Sie in der Cloud hochladen wollen und welches Risiko mit einer Speicherung verbunden ist. Bei besonderen rechtlichen Vorgaben sollten die Daten innerhalb der Schweiz gelagert werden. Es ist empfehlenswert, sensible Daten nicht oder nur verschlüsselt in der Cloud zu speichern. Überprüfen Sie in diesem Zusammenhang auch die Freigaberechte, wenn Sie Ihre Daten teilen möchten , zum Beispiel restriktiv oder zeitlich beschränkt, und wie einfach es ist, Ihre Daten wieder aus der Cloud zu entfernen, falls Sie künftig den Dienst wechseln möchten.

Beachten Sie, dass die Cloud ein Online-Speichermedium ist und daher ebenfalls von einem Cyberangriff betroffen sein kann. Clouddienste schützen sich nur bedingt vor Angriffen mit Verschlüsselungs-Schadsoftware (Ransomware). Falls die Daten ausschliesslich in der Cloud abgelegt sind, werden bei einem Angriff unter Umständen auch diese Daten verschlüsselt. Der Schutz hängt vor allem davon ab, ob die Dienste eine Wiederherstellung zu früheren Versionen bieten und ob dieser Zugriff besonders geschützt ist, so mindestens durch ein sicheres Passwort und eine Zweifaktor-Authentifizierung.

Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte
www.edoeb.admin.ch

Bundesamt für Sicherheit in der Informationstechnik Deutschland
www.bsi.bund.de

Konferenz der Schweizer Daten-schutz-Beauftragten Privatim
www.privatim.ch

Agentur der Europäischen Union für Cybersicherheit
www.enisa.europa.eu

3.3 Bleiben Sie technisch gewappnet

Grundlegende Sicherheitseinstellungen

Installieren Sie auf jedem Computer einen Virenschutz und aktivieren Sie den Echtzeitschutz. Sorgen Sie dafür, dass sich dieser regelmässig aktualisiert und täglich einen vollständigen Systemscan durchführt.

Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware. Stellen Sie sicher, dass Ihre Systeme auf dem aktuellen Stand sind (Updates). Das gilt auch für alle Programme und Apps sowie für Content Management Systeme (CMS) Ihres Web-Auftritts.

Auf jedem Computer sollten Sie eine Personal Firewall verwenden. Schützen Sie zudem Ihr Unternehmensnetzwerk mit einer Firewall vor unerwünschten Verbindungen mit dem Internet. Standardmässig sollte die Firewall sämtlichen Verkehr blockieren, ausser den durch Regeln freigegebenen Datenverkehr.

Schwachstellenmanagement

Stellen Sie sicher, dass Auffälligkeiten und sicherheitsrelevante Ereignisse zeitgerecht erkannt werden. Überwachen Sie Ihre Netzwerkinfrastruktur, beispielsweise mit einem Angriffserkennungs-System (IDS) und Angriffsschutz-System (IPS). Teilweise sind diese auch in Web-Proxy-Services enthalten.

Definieren Sie, welche Log-Dateien (Ereignisprotokolldateien) gespeichert werden und wie lange. Eine Analyse der Log-Dateien bringt Erkenntnisse über Stabilität und Verfügbarkeit der Netzwerke, Systeme und Anwendungen. Zudem helfen sie den Ursprung eines Angriffs zu erkennen, Informationen über infizierte Systeme im eigenen Netzwerk zu erhalten und geeignete Gegenmassnahmen zu ergreifen. Im Zusammenhang mit der Speicherung und Analyse von Log-Files sind zwingend datenschutzrechtliche Aspekte zu beachten.

Tipp: Einfach und umfassend

Bei vielen neuen Betriebssystemen sind diverse Sicherheitsfunktionen, wie beispielsweise Firewall- und Netzwerkschutz, Viren- und Bedrohungsschutz oder automatische Updates, bereits integriert. Aktivieren Sie die entsprechenden Funktionen für sämtliche Geräte in Ihrem Netzwerk.

All-in-one-Lösungen bieten beispielsweise sogenannte Unified-Threat-Management-Systeme. Diese umfassende Sicherheitslösung gibt es als Hardware-, Software- oder Cloudlösung.

Erweiterte Websicherheit

Nutzen Sie weitere Web-Sicherheitskomponenten, wie beispielsweise ein DNS-Filtering («Domain Name System») und einen Web-Proxy, der bekannte schädliche Websites sperrt beziehungsweise nur den Zugriff auf als sicher eingestufte Websites erlaubt («Whitelist»). So werden Anfragen zu kriminellen Webseiten unterbunden und die Privatsphäre Ihres Unternehmens geschützt.

Wenn Sie ein Programm aus dem Internet herunterladen möchten, informieren Sie sich zuerst über die Seriosität des Anbieters und der entsprechenden Software. Hierbei sollten Hashwerte und Signaturen der Software gemäss Herstellerangaben überprüft werden. Laden Sie Software nur von der Website des Herstellers herunter.

Netzwerksegmentierung

Segmentieren Sie Ihr Unternehmensnetz in einzelne Bereiche («Netzwerksegmentierung»), etwa separate Netze für Produktion, Personal, Buchhaltung usw. So vermeiden Sie, dass beispielsweise Steuerungscomputer von Werksanlagen, die nicht mehr aktualisiert werden können, zum Einfallstor für Angreifende werden und Ihr gesamtes Netzwerk gefährden.
Verwenden Sie auch einen separaten Verzeichnisdienst für Ihr Backup. Dies kann verhindern, dass Kriminelle, die sich bereits in Ihrem System befinden, Zugang zu Ihrem Backup erhalten.

Fernzugriffe (Remote Access)

Schützen Sie Fernzugriffe auf Ihr Netzwerk mit Benutzername, Passwort und einer Zwei-Faktor-Authentisierung. Setzen Sie eine sichere Verbindung über ein virtuelles privates Netzwerk (VPN) ein – auch für den Zugriff von Administratoren und externen IKT-Dienstleistungsunternehmen. Es empfiehlt sich, Fernwartungszugänge nur dann zu öffnen, wenn sie benötigt werden.

Gefährliche Anhänge und Makros

Häufig gelangen elektronische Schädlinge durch E-Mail-Anhänge, getarnt als angebliche Rechnungen oder Bewerbungen, auf Ihren Computer. Potenziell schädliche E-Mail Anhänge sollten deshalb bereits auf Ihrem E-Mail-Gateway beziehungsweise Spam-Filter blockiert werden.
Eine ausführliche, aktualisierte Liste solch gefährlicher Anhänge finden Sie auf der Website des BACS, https://www.ncsc.admin.ch/govcert#1737483390 .

Deaktivieren Sie Office-Makros, wenn Sie diese nicht verwenden. Stellen Sie sicher, dass keine Makros in Office-Dokumenten unsicherer Herkunft ausgeführt werden können. Sensibilisieren Sie Ihre Mitarbeitenden dahingehend, dass entsprechende Warnhinweise in Office-Programmen nicht ignoriert werden dürfen.

Tipp: Ist mein Gerät von einer Schadsoftware befallen?

Haben Sie den Verdacht, dass Sie eine Schadsoftware heruntergeladen haben oder dass sich Kriminelle auf Ihrem Gerät befinden? Achten Sie auf folgende Warnzeichen:

- Sie erhalten unerwartete Meldungen, Bilder oder Tonsignale;
- Ihre Antivirus-Programm meldet eine Gefahr;
- Programme werden geöffnet oder stellen eigenständig eine Internetverbindung her;
- Dateien verschwinden oder werden geändert;
- Von Ihrem Konto aus werden Nachrichten an Personen aus Ihrem Umfeld verschickt;
- In Ihrem Postfach befinden sich Nachrichten ohne Absender oder Betreff;
- Ihr Computer ist eingeschaltet, aber das Betriebssystem fährt nicht hoch, ist langsam und/oder stürzt ab;
- Der Browser friert ein oder erscheint Ihnen seltsam.

Melden Sie den Verdacht umgehend Ihrer IKT-Fachperson und lassen Sie Ihr Gerät überprüfen.

3.4 Sichern Sie Ihre Daten

Stellen Sie sicher, dass Sicherungen (Backups) Ihrer Informationen regelmässig durchgeführt, bewirtschaftet und getestet werden (Rückspielbarkeit der Backups testen). Lagern Sie eine zusätzliche Kopie Ihres Backups offline, beispielsweise auf einer externen Festplatte, und ausser Haus. So kann unter anderem sichergestellt werden, dass bei einem Ransomware-Angriff und der darauffolgenden Verschlüsselung der Daten eine funktionstüchtige Sicherungskopie vorhanden ist. Hintergrund der Offsite-Lagerung ist auch, dass diese vor Diebstahl, Feuer und Wasser geschützt ist.

Tipp: Sicherheitskontakt auf Ihrer Webseite hinterlegen

Bei Cybersicherheitsproblemen ist eine schnelle Kontaktaufnahme durch die Strafverfolgungsbehörden oder Sicherheitsdienstleister/-in mit dem zuständigen Sicherheitskontakt sehr wichtig. Mit dem Standard «security.txt» steht eine Möglichkeit zur Verfügung, den Sicherheitskontakt einheitlich auf Ihrer Webseite zu publizieren und somit schneller aufzufinden. Einen Leitfaden hierfür finden Sie auf der Webseite des Bundesamts für Cybersicherheit:

https://www.ncsc.admin.ch/23-stxt-de

3.5 Seien Sie auf einen Angriff vorbereitet

Erarbeiten Sie eine Risikostrategie für den Ereignisfall. Legen Sie die Prioritäten, Einschränkungen und maximal tragbaren Risiken fest. Stellen Sie sich darauf ein, dass Sie nach einem Vorfall während Tagen Teile Ihrer Dienstleistung nicht erbringen können oder Ihre Produktionsanlagen stillstehen. Eingespielte Prozesse und Eskalationspfade sind deshalb unabdingbar, um die Kontrolle bei einem Vorfall zu behalten. Führen Sie Notfallübungen durch. Richten Sie ein geeignetes Krisenmanagement ein. Empfehlenswert ist auch, ein Konzept für die öffentliche Kommunikation bereit zu haben.

Die Zusammenarbeit mit Partnerunternehmen sollte ebenfalls in Ihre Sicherheitsüberlegungen miteinfliessen. Die Kettenreaktion, die möglicherweise durch einen erfolgreichen Angriff auf ein Partnerunternehmen ausgelöst wird, kann die gesamte Wertschöpfungskette und damit auch Ihr Unternehmen gefährden.

Mitarbeitende sind für mögliche Anzeichen eines Vorfalls zu sensibilisieren und darüber in Kenntnis zu setzen, an wen sie entsprechende Feststellungen melden sollen.

Weitere Informationen zum strategischen und operativen Risikomanagement finden Sie auf dem KMU-Portal des Bundes: https://www.kmu.admin.ch/. Das Bundesamt für Bevölkerungsschutz hat einen Leitfaden zum Schutz kritischer Infrastrukturen erarbeitet: https://www.babs.admin.ch/de/aufgabenbabs/ski/leitfaden.html. Dieser basiert auf gängigen Normen und Standards im Bereich Risiko-, Notfall-, Krisen- und Kontinuitätsmanagement. Die Effekte von Cybergefahren werden dabei berücksichtigt. Der Leitfaden kann auch für Unternehmen, die nicht als kritische Infrastruktur gelten, bei der Erarbeitung einer Risikostrategie hilfreich sein.

3.6 Bleiben Sie informiert

Informieren Sie sich regelmässig über die aktuellen Vorgehensweisen von Cyberkriminellen und lernen Sie entsprechende Schutzmassnahmen kennen. Mit folgenden Websites bleiben Sie auf dem Laufenden:

Kantonspolizei Bern

www.police.be.ch/cyber

Bundesamt für Cybersicherheit (BACS)

www.ncsc.admin.ch

Cybercrimepolice

www.cybercrimepolice.ch

iBarry

www.ibarry.ch

Card Security

www.card-security.ch

Schweizerische Kriminalprävention (SKP)

www.skppsc.ch

Stellen Sie sicher, dass Ihre Mitarbeitenden regelmässig bezüglich aller Belange der Cybersicherheit angemessen und stufengerecht geschult sind. Vergessen Sie auf keinen Fall Angestellte im Praktikum, Lernende und Teilzeitmitarbeitende. Erläutern Sie die Notwendigkeit der Sicherheitsmassnahmen und den korrekten Umgang mit definierten Richtlinien, zum Beispiel Weitergabe von Informationen oder Passwortregeln.

Tipp: Darauf können Ihre Mitarbeitenden achten

Klicken Sie in verdächtigen Nachrichten (Mails, SMS, Messaging-App) nicht auf Anhänge und Links.

Geben Sie keine vertraulichen Informationen und Daten über unpersönliche Kanäle oder an Unbekannte preis. Gewähren Sie auch keinen Zugriff auf Ihren Computer.

Öffentliche Internetverbindungen (auch passwortgeschützte) sind generell nicht sicher. Übermitteln Sie vertrauliche Informationen nur über Verbindungen, welche zusätzlich mit einem Virtual Private Network (VPN) geschützt sind. Sie können auch eine 3G/4G/5G-Datenübertragung via Roaming verwenden, um auf das Internet zuzugreifen.

Lassen Sie Ihr Material, Ihre Dokumente oder Geräte nie unbeaufsichtigt liegen.

Fahren Sie Ihren Computer nach Arbeiten durch IKT-Fachpersonen herunter. Sonst bleibt der Admin-Account aktiv.

Verwenden Sie sichere Passwörter mit mindestens zwölf Zeichen, Gross- und Klein-buchstaben, Zahlen und Sonderzeichen, die zufällig generiert wurden. Ganz wichtig: Jede Anwendung muss ein eigenes Passwort haben! Ergänzen Sie Ihr Passwort mit einer Zwei-Faktor-Authentifizierung, zum Beispiel SMS-Code.

4_Was Sie bei einer Auslagerung der IKT-Leistungen beachten sollten

Falls Sie Ihre IKT-Infrastruktur auslagern und Ihre IKT durch eine oder mehrere externe Firmen betrieben wird, finden Sie nachfolgend einige Tipps. Beachten Sie jedoch, dass die Verantwortung nicht ausgelagert oder delegiert werden kann. Bei einem Vorfall kann Ihr Unternehmen am Ende der Haftungskette stehen.

Mindestanforderungen

Bereits bei der Abnahme integrierter IKT-Systeme sind Sicherheitsprüfungen durchzuführen. Informieren Sie sich über relevante Allgemeine Geschäftsbedingungen (AGB) und Vorgaben bei Inanspruchnahme von Informatikleistungen. Diese Vorgaben sollten Bestandteil der Vertragsverhältnisse zwischen Ihnen und den externen IKT-Dienstleistungsunternehmen sein. Die gesetzlichen Geheimhaltungspflichten für Wartung und Betreuung von IKT-Systemen durch Dritte sind zu regeln und unnötiger Zugang zu besonders schützenswerten Personendaten ist nicht zu gestatten. Abklärungen und Vereinbarungen sind auch mit dem jeweiligen Unternehmen für die Datenspeicherung (Cloud-Unternehmen) vorzunehmen und zu treffen.

Scheuen Sie sich nicht vor persönlichen Rückfragen, wenn Ihnen etwas ungewöhnlich vorkommt – auch bei bekannten Absender/-innen! Wählen Sie nicht die Telefonnummer aus der suspekten Nachricht. Suchen Sie die Kontaktangaben auf der offiziellen Website, indem Sie die Originaladresse selbst im Browser eintippen. Vorsicht auch beim «Antworten»-Knopf: schreiben Sie die E-Mail-Adresse neu.

Melden Sie verdächtige Vorkommnisse Ihrer IKT-Fachperson.

Sicherheitsaudits

Die Umsetzung der im Vertrag festgehaltenen Leistungen muss periodisch nach anerkannten Auditstandards, beispielsweise auf Basis von COBIT (Control Objectives for Information and Related Technology) der Information Systems Audit and Control Association (ISACA), kontrolliert werden. Nehmen Sie dafür die Dienste unabhängiger Prüfstellen in Anspruch. Das IKT-Dienstleistungsunternehmen kann auch ein sogenanntes ISAE 3402 Type 2 (International Standard on Assurance Engagements) machen lassen – auch bekannt als SOC-2-Bericht (Service Organization Control). Die Prüfstelle bewertet Aspekte von Sicherheit, Verfügbarkeit, Integrität und Vertraulichkeit.

Qualifikationen

Zertifizierungen nach anerkannten Datenschutz- und Informationssicherheitsstandards oder Kontrollberichte von unabhängigen Dritten können bei der Auswahl des Unternehmens behilflich sein. Sie müssen nicht zwingend zertifizierte Partner auswählen. Empfehlenswert ist es, wenn IKT-Dienstleistungsunternehmen aufzeigen können, dass sie Ihren gestellten Anforderungen entsprechen, sowie die von Ihnen geforderte Verfügbarkeit und Sicherheit gewährleisten können. Lassen Sie dies durch eine unabhängige Stelle prüfen oder bestätigen.

Es existiert eine Vielzahl unterschiedlicher Standards und Leitfäden. IKT-Dienstleistungsunternehmen sollten mit den Standards ISO 27001, ISO 22301, ISO 9001, ISO 14001 und NIST vertraut und konform sein. Werden andere verwendet, hat das Unternehmen ein Compliance Mapping nachzuweisen. Sollten Sie einen erhöhten Schutzbedarf haben, müssen Sie eigene weitergehende Anforderungen formulieren.

5_Wie Sie Cyberangriffe bewältigen

Werden Sie angegriffen, müssen Sie schnell handeln. Gehen Sie wie folgt vor:

Isolieren
Trennen Sie infizierte Systeme umgehend vom Netz. Das heisst: Netzwerkkabel von den betroffenen Geräten ziehen und WLAN ausschalten.

Kontaktieren

Kontaktieren Sie Ihre IKT-Ansprechperson.

Kontaktieren Sie die örtlich zuständige Polizei. Befinden Sie sich in einer Notlage, wählen Sie die Notrufnummer 112.

Sprechen Sie die weiteren Schritte mit der Polizei ab. Setzen Sie betroffene Geräte und Systeme möglichst erst nach der Spurensicherung durch die Polizei neu auf.

Informieren Sie Ihre Partnerunternehmen und Kunden über den Vorfall, da sie eventuell selbst betroffen sind.

Beachten Sie auch die Meldepflichten, zum Beispiel bezüglich des Datenschutzes.

Bewältigen
Setzen Sie Ihr Krisenkonzept um. Berufen Sie den Krisenstab ein und überlassen Sie die Kommunikation den Fachpersonen.

5.1 Melden Sie einen Vorfall – mit oder ohne Schaden

Vorfälle mit Schaden

Bei einem Angriff auf IKT-Systeme werden in der Regel mehrere Straftaten begangen, zum Beispiel unbefugte Datenbeschaffung oder unbefugtes Eindringen in ein Datenverarbeitungssystem, Betrug oder Erpressung. Kontaktieren Sie in diesem Fall die Polizei oder die Staatsanwaltschaft und erstatten Sie Anzeige.

Vorfälle ohne Schaden

Melden Sie erfolglose Cyberangriffe oder Betrugsversuche ohne Schaden online beim BACS (report.ncsc.admin.ch). Jede Meldung hilft dabei, die Aktivitäten von Kriminellen im Internet zu verfolgen und auf Angriffswellen frühzeitig reagieren zu können. Informelle Hinweise an das BACS können jedoch nicht für eine Anklage respektive in einem Gerichtsverfahren verwendet werden.

5.2 Weshalb sich der Gang zur Polizei lohnt

Die Polizei ist sich der heiklen und stressigen Situation für ein Unternehmen bewusst. Deshalb ist sie bestrebt, diskret und schnell vorzugehen. Die Untersuchung unterliegt dem Amtsgeheimnis. Auf Ihre Infrastruktur wird nicht eingewirkt und der allenfalls noch laufende Betrieb nicht gestört. Bei einem Angriff sucht die Polizei nur nach Informationen und Spuren, die für die Aufklärung der Straftat relevant sind. Während der Ermittlung erhalten Sie wichtige Informationen, die helfen, das Ereignis schneller zu bewältigen oder die verhindern, dass wertvolle Unternehmensinformationen weiter abfliessen. Sie erfahren, wie die Täterschaft vorgegangen ist beziehungsweise wo die Sicherheitslücke war. Bei einer Lösegeldforderung werden Sie fachkundig unterstützt. Die Strafverfolgungsmassnahmen werden mit Ihnen abgesprochen – Sie können jederzeit Ihren rechtlichen Fachbeistand einbeziehen.

Im Gegenzug können Sie der Polizei auch Informationen zum Schutz anderer Unternehmen liefern: Anonymisierte Erkenntnisse aus Strafverfahren dienen der Optimierung bestehender und Entwicklung neuer Präventions- und Bekämpfungsstrategien.

6_Holen Sie sich Unterstützung

Diverse Stellen bieten relevante Informationen zur IKT-Sicherheit, Hilfsmittel und / oder Unterstützung an:

Kantonale und städtische Polizeikorps

Diverse Polizeikorps der Schweiz bieten sachkundige Informationen zum Thema Cybercrime-Prävention an. Bei Interesse wenden Sie sich an die verantwortliche Fachabteilung des örtlich zuständigen Polizeikorps.

Bundesamt für Cybersicherheit (BACS)

Das Bundesamt für Cybersicherheit, www.ncsc.ch, ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Sollte Ihr Unternehmen zu den kritischen Infrastrukturen gehören, aber noch nicht Mitglied des BACS sein, wenden Sie sich an outreach@ncsc.ch.

Nachrichtendienst des Bundes (NDB)

Der NDB hilft in Zusammenarbeit mit den Kantonalen Nachrichtendiensten die Unternehmen, Hochschulen und Forschungseinrichtungen über Proliferation und Spionage aufzuklären, zu sensibilisieren und zu beraten (www.ndb.admin.ch oder prophylax@ndb.admin.ch). Auf der Webseite des NDB befindet sich eine Broschüre zum Thema mit entsprechenden Schutzempfehlungen.

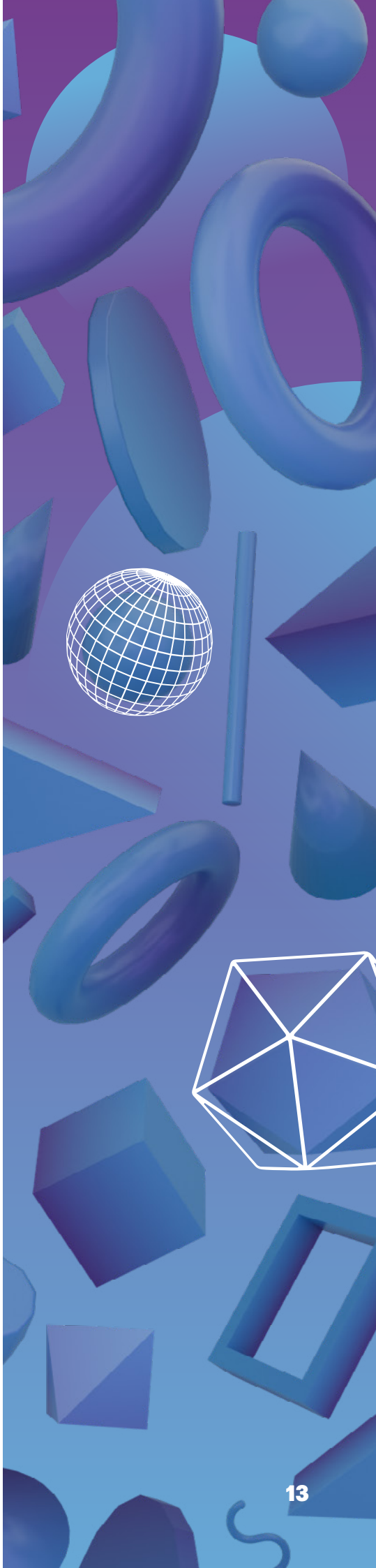
Bundesamt für wirtschaftliche Landesversorgung (BWL)

Das BWL hat Minimalstandards für IKT sowie ein Assessment-Tool ausgearbeitet. Betreibern von kritischen Infrastrukturen wird empfohlen, den IKT-Minimalstandard umzusetzen. Die Standards bieten jedoch grundsätzlich jedem interessierten Unternehmen oder jeder Organisation eine Hilfestellung und konkrete Handlungsanweisungen zur Verbesserung der eigenen IKT-Resilienz. Mit dem Assessment-Tool können Sie den Umsetzungsstand der Schutzmassnahmen beurteilen respektive durch externe Firmen prüfen lassen (Audit). Diese finden Sie unter: www.bwl.admin.ch.

Datenschutz

Seit dem 1. September 2023 gibt es in der Schweiz ein neues Gesetz für den Schutz der Daten der Bevölkerung. Als Unternehmen müssen Sie Ihre Bearbeitung von Personendaten an diese Bestimmungen anpassen. Für die Bearbeitung von Personendaten durch Private und durch Bundesorgane ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) zuständig, www.edoeb.admin.ch. Im KMU-Portal des Bundes www.kmu.admin.ch finden Sie Informationen zum Thema Datenschutz.

Hilfsmittel zum Datenschutz und eine Auflistung der jeweiligen Datenschutzaufsichtsstellen sind auf der Website der Konferenz der schweizerischen Datenschutzbeauftragten, privatim, www.privatim.ch, publiziert.



7_Anhänge

7.1 Checkliste: Kurzbeurteilung Ihrer Cybersicherheit

Diese Checkliste hilft Ihnen, sich mit den wichtigsten Fragen zu einem minimalen Cyberschutz auseinanderzusetzen. Nehmen Sie bei jedem «unklar» oder bei einem «nein» entsprechende Abklärungen vor.
Falls Sie Ihre IT ausgelagert haben, prüfen Sie, ob die nachstehenden Punkte im Vertrag mit dem Dienstleistungsunternehmen abgedeckt sind.

Füllen Sie diese Cyberkurzbeurteilung auch für allfällige Tochterunternehmen und die für das Unternehmen zentralen Zulieferer aus. Empfehlenswert ist ausserdem der Austausch mit den wichtigsten Partnerunternehmen, da Cybervorfälle auch Auswirkungen auf die gesamte Wertschöpfungskette haben können.

Auf der Website des Bundesamtes für wirtschaftliche Landesversorgung www.bwl.admin.ch finden Sie ein detailliertes Assessment-Tool für die IKT-Minimalstandards. Damit können Sie den Umsetzungsstand der Schutzmassnahmen beurteilen respektive durch externe Firmen prüfen lassen (Audit).

Überprüfen Sie die Punkte auf der Checkliste regelmässig, denn Cybersicherheit ist eine Daueraufgabe.

Organisation und Prozesse	Ja	Nein	Unklar
Ist in Ihrem Unternehmen bestimmt, wer für Cybersicherheit verantwortlich ist?	☐	☐	☐
Haben Sie bereits Cyber-Risikobewertungen durchgeführt?	☐	☐	☐
Wurden die wesentlichen Cyberrisiken identifiziert, werden diese überwacht und dokumentiert?	☐	☐	☐
Wissen Sie, wie Ihre IKT-Landschaft aussieht, zum Beispiel Inventar, Softwares, relevante externe IKT-Systeme?	☐	☐	☐
Haben Sie einen Notfallplan sowie ein Kommunikationskonzept für den Fall, dass Sie von einem Cyberangriff betroffen sind?	☐	☐	☐
Ist der physische Zugang zur Rechner-, Server- und Netzwerkinfrastruktur sowie Datenleitungen vor dem Zugriff von Dritten geschützt?	☐	☐	☐
Sensibilisierung von Mitarbeitenden			
Werden die Mitarbeitenden regelmässig bezüglich Cybersicherheit geschult?	☐	☐	☐
Erhalten Geschäftsleitung und Mitarbeitende mit Überweisungskompetenz oder Zugang zu sensiblen Daten funktionsgerechte Trainings?	☐	☐	☐
Sind die Mitarbeitenden mit den Unternehmensrichtlinien vertraut?	☐	☐	☐
Schutz der Daten			
Ist eine interne Datenschutzrichtlinie / Informationssicherheitspolitik vorhanden und sind die Mitarbeitenden damit vertraut?	☐	☐	☐
Werden die aktuell geltenden Vorschriften zum Datenschutz, zur Datenspeicherung und Datenverarbeitung konsequent und korrekt umgesetzt?	☐	☐	☐

Zugangskontrolle und Rechte	Ja	Nein	Unklar
Haben Sie ein Berechtigungs- und Rollenkonzept für die Mitarbeitenden (Zugang nur zu funktionsrelevanten Informationen)?	☐	☐	☐
Sind lokale Administratorenrechte auf Mitarbeiterarbeitsplätzen gesperrt?	☐	☐	☐
Verfügen Sie über eine Passwortrichtlinie und setzen Sie starke Authentisierungsverfahren ein?	☐	☐	☐
Geschütztes Netzwerk			
Sind die einzelnen Bereiche Ihres Unternehmens, zum Beispiel Personal und Buchhaltung, getrennt (Netzwerksegmentierung) und die Zugriffe geregelt? Alternative für Kleinstunternehmen: Verwenden Sie einen separaten Computer oder ein separates System für unterschiedliche Bereiche, zum Beispiel Büro, Personal und E-Banking?	☐	☐	☐
Ist in Ihrem Unternehmen der externe Zugang (Fernzugriff) zur Rechner-, Server- und Netzwerkinfrastruktur sowie zur Cloud geschützt (VPN, Zwei-Faktor-Authentisierung) und kann dieser bei nicht Verwendung getrennt werden (kontrollierte Zugänge)?	☐	☐	☐
Ist im E-Mail-Programm definiert, welche Anhänge als potenziell gefährlich gelten und ist die Ausführung von Makros in Office-Dokumenten geregelt?	☐	☐	☐
Benutzen Sie veraltete Software und / oder Hardware, welche offiziell nicht mehr mit Sicherheits-Updates unterstützt werden?	☐	☐	☐
Spielen Sie zeitnah Korrekturen (sicherheitskritische Patches und Updates) für Ihre IKT-Systeme und Software ein?	☐	☐	☐
Verwenden Sie Antivirus, Antispyware oder gleichwertigen Schutz vor Schadprogrammen?	☐	☐	☐
Verfügen Sie über einen Prozess, um Schwachstellen in Ihrer Software oder Ihren IKT-Systemen zu erkennen, damit Massnahmen ergriffen und deren Behandlung möglich werden können, zum Beispiel IPS, IDS, Logserver?	☐	☐	☐
Werden alle Internet-Zugangspunkte durch Firewalls geschützt?	☐	☐	☐
Betreiben Sie verschlüsselte Drahtlosnetzwerke?	☐	☐	☐
Nutzen Sie erweiterte Web-Sicherheitskomponenten wie beispielsweise ein DNS-Filtering («Domain Name System») und einen Web-Proxy?	☐	☐	☐
Backup			
Werden regelmässig Datensicherungen durchgeführt, bewirtschaftet und getestet (Rückspielbarkeit)?	☐	☐	☐
Wird eine zusätzliche Kopie des Backups getrennt (offline) sowie eine ausserhalb des Rechenzentrum-Standortes (offsite, zum Beispiel Cloud, Bankschliessfach) aufbewahrt?	☐	☐	☐
Verwenden Sie einen separaten Verzeichnisdienst für Ihr Backup?	☐	☐	☐
Vertrag mit dem IT- und Cloud-Dienstleistungsunternehmen			
Ist die Haftung in einem Schadensfall und sind die Ausschlüsse der Leistungsverpflichtung, beispielsweise höhere Gewalt, vertraglich geregelt?	☐	☐	☐
Sind die Servicelevel für Regel- und Notbetrieb eindeutig formuliert?	☐	☐	☐
Ist die Exit-Strategie durchdacht und vertraglich festgehalten, insbesondere bei Cloud-Lösungen?	☐	☐	☐
Zusammenarbeit mit den Strafverfolgungsbehörden			
Sind die verantwortliche Person sowie die Ansprechperson im Falle eines Vorfalls definiert und verfügbar?	☐	☐	☐

7.2 Zertifizierungen, Standards und Leitfäden

Es existiert eine Vielzahl verschiedener Standards und Zertifikate mit verschiedenen Schwerpunkten. Je nachdem, wie die eigenen Bedürfnisse sind, können unterschiedliche Standards oder Zertifikate bei der Auswahl herangezogen werden. Einige Beispiele:

Krisenmanagement, Business Continuity, Disaster Recovery

ISO 22301, Business Continuity Management System
ISO 27031, IT Service Continuity Management System
BS 11200, Krisenmanagement-System

Daten- und Informationssicherheit

ISO 27001, Informationssicherheit
ISO 27701, Erweiterung von ISO 27001 um Datenschutz
ISO 30141, Referenzarchitektur für das Internet der Dinge (IoT), Vertraulichkeit der verarbeiteten Daten
Ausrichtung gemäss Verordnung der EU 2016/679, Datenschutz-Grundverordnung (DSGVO)
NIST Cybersecurity Framework

Technische Leitfäden

EN 50173, Verkabelungsstruktur
EN 50600, Rechenzentren
ANSI/TIA-942, Rechenzentren
IEC 62443, Technische Anforderungen der Industrienorm

Cloud

ISO 27017, Verhaltenskodex für Informationssicherheitskontrollen (basierend auf ISO/IEC 27002, Leitfaden für Informationssicherheitsmassnahmen)
ISO 27018, Verhaltenskodex zum Schutz von personenbezogenen Daten in der Cloud

Andere (v.a. für Hardwarelieferanten)

ISO 9001, Qualitätsmanagement
ISO 14001, Umweltmanagement

Leitfäden für Auftraggebende

ISO 22300, Terminologienorm zu Sicherheit und Resilienz
ISO 22318, Supply Chain Continuity
ISO 27036, Informationssicherheit im Lieferantenmanagement
ISO 31010, Risikomanagement

Es gibt Akteure, die Zertifizierungen ohne Akkreditierung anbieten.
Die Schweizerische Akkreditierungsstelle SAS begutachtet und akkreditiert Konformitätsbewertungsstellen.

(KBS). Hier kann gesucht werden, welche Zertifizierungsstelle für welche Normen zugelassen ist:
Suche akkreditierte Stellen SAS.

Impressum
Inhalt: Kantonspolizei Bern, Fachstelle Projekte und Cybercrime, im Auftrag des Netzwerks Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK). In Zusammenarbeit mit dem Bundesamt für Cybersicherheit (BACS) und dem Bundesamt für wirtschaftliche Landesversorgung (BWL).

Gestaltung und Layout: NEDIK

Kontakt: praevention@police.be.ch, Tel: 031 638 91 00

NEDIK

POLICE

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung BWL

Bundesamt für Cybersicherheit BACS