Bestandsaufnahme und Bedarfsanalyse für IT-Sicherheitskonzepte

Kurzbeschreibung

Anhand von neun Checklisten können Sie für alle wichtigen Bereiche der IT-Sicherheit Ihren aktuellen Sicherheitsstatus feststellen, Schutzlücken erkennen und auf dieser Basis ein IT-Sicherheitskonzept entwickeln.

Vorbemerkung

IT-Sicherheit muss sein: Nicht nur in börsennotierten Unternehmen, sondern auch in GmbHs, AGs und anderen Kapitalgesellschaften sind Vorstände und Geschäftsführer für die IT-Sicherheit persönlich haftbar. Der Gesetzgeber schreibt außerdem die Rechtskonformität sämtlicher Unternehmensabläufe vor. Wichtigster Bestandteil ist dabei die "IT-Compliance", deren zentrales Element wiederum die IT-Sicherheit ist. Und dann sind da ja auch noch die Banken und die ISO-Zertifizierung, die auch angemessene IT-Sicherheitsvorkehrungen verlangen. Doch was ist angemessen? Mit unseren Checklisten können Sie die vorhandenen Sicherheitsmaßnahmen prüfen und Ihr eigenes Sicherheitskonzept optimieren. Weitere Informationen lesen Sie im Fachbeitrag IT-Sicherheit: PraxisCheck zur Bestandsaufnahme und Bedarfsanalyse

Hinweis

Die Fragenkataloge der Checklisten können Sie auch in elektronischer Form mit unserem PraxisCheck beantworten. Als Ergebnis erhalten Sie eine detaillierte Auswertung für weitere Maßnahmen.

Checklisten-Überblick

Die folgenden Checklisten fassen die wichtigsten IT-Sicherheitsanforderungen und -maßnahmen in kurzen Fragen zusammen, die Sie nur mit **Ja**, **Nein** oder **Prüfen** zu beantworten brauchen. Anhand Ihrer Antworten erhalten Sie ein sehr genaues Bild über den aktuellen Zustand und über die Schwachstellen der IT-Sicherheit und die IT-Compliance in Ihrem Unternehmen.

Die Checklisten entsprechen den Sicherheitskriterien, die im IT-Grundschutzkatalog festgelegt sind, das vom **Bundesamt für die Sicherheit in der Informationstechnik (BSI)** herausgegeben und über das Internet kostenlos zur Verfügung gestellt wird (www.bsi.bund.de).

Die Fragenkataloge der Checklisten sind in folgende Sicherheitsbereiche unterteilt:

Checkliste 1 : Sicherheitsmanagement

Im betrieblichen Umfeld ist das IT-Sicherheitsmanagement in jedem Fall Chefsache. Und dies nicht nur, weil das Thema **Sicherheit** von entscheidender Bedeutung für den Geschäftserfolg ist, sondern weil dies auch vom Gesetzgeber so vorgesehen ist. Natürlich müssen Geschäftsführer und Firmenleitung sich nicht persönlich um die Details der Umsetzung von Sicherheitskonzepten und Sicherheitsrichtlinien kümmern. Sie müssen aber den Rahmen dafür schaffen, Verantwortung übernehmen und qualifizierte Verantwortliche einsetzen und - in letzter Konsequenz- persönlich haften.

Checkliste 2: Allgemeine Sicherheitsaspekte und Verhalten in Notfällen

Es gibt eine ganze Reihe allgemeiner Sicherheitsaspekte, die bei jeder Art der Nutzung der vorhandenen Computer- und Kommunikationseinrichtungen berücksichtigt werden sollten. Da es sich dabei vor allem um die konkrete Umsetzung von Sicherheitsmaßnahmen handelt, sind hier neben der Geschäftsleitung

auch alle IT-Verantwortlichen angesprochen. Schutzmechanismen und programminterne Sicherheitseinrichtungen, aber auch konkrete Handlungsanweisungen helfen dabei, Sicherheitsrisiken zu minimieren und Datensicherheit zu gewährleisten.

Checkliste 3: Sicherheitsbewusstsein

Die Aufrechterhaltung des Sicherheitsniveaus ist genauso wichtig wie die Einführung angemessener Sicherheitsmaßnahmen. Die besten Sicherheitseinrichtungen und -maßnahmen nützen aber überhaupt nichts, wenn diese nicht ein- und umgesetzt werden. Nur wenn Mitarbeiter positiv motiviert sind und einsehen, warum bestimmte Sicherheitsmaßnahmen sie einschränken oder von ihnen selbst immer wieder aktiv durchgeführt werden müssen, kann ein IT-Sicherheitskonzept auf Dauer erfolgreich umgesetzt werden.

Checkliste 4: Zugriffsschutz: Benutzernamen, Kennwörter und Verschlüsselung

Der Zugriffsschutz und die damit verbundene Zugriffskontrolle sind für die IT-Sicherheit ebenfalls von entscheidender Bedeutung. Benutzernamen, Passwörter, Kennwörter und Verschlüsselungsverfahren sorgen dafür, dass bestimmte elektronische Informationen nur von befugten Mitarbeitern eingesehen und tatsächlich vertraulich verwendet werden können. Um sicherzustellen, dass bestimmte IT-Komponenten und Daten auch noch dann zur Verfügung stehen, wenn bestimmte Mitarbeiter ausfallen oder für längere Zeit nicht erreichbar sind, sollten alle gültigen Kenn- und Passwörter außerdem hinterlegt und sicher verwahrt werden.

Checkliste 5: Internet und E-Mail

Internetanbindung und E-Mail-Kommunikation sind aus dem betrieblichen Alltag nicht mehr wegzudenken, stellen aber gleichzeitig eine große Sicherheitsbedrohung dar. Jeder Mitarbeiter, der im Internet surft und E-Mails versendet und empfängt, macht nicht nur seinen Arbeitsplatzrechner, sondern gleichzeitig auch das gesamte Computersystem, mit dem der Arbeitsplatzrechner verbunden ist, zum potenziellen Ziel von Viren und anderen Schadprogrammen und öffnet es für potenzielle Eindringlinge. Jede Art der Internetverbindung muss daher mit allen zur Verfügung stehenden Mitteln geschützt werden.

Checkliste 6: Datensicherung

Da auch die besten Sicherheitsmaßnahmen Naturkatastrophen, Brandschäden oder gezielten Vandalismus nicht ausschließen können, ist die regelmäßige Datensicherung immer noch eine unverzichtbare Risikovorsorge. Dazu gehört aber auch, dass Vorkehrungen dafür geschaffen werden, dass die gesicherten Daten außer Haus gelagert werden.

Checkliste 7: Drahtlose Netzwerkverbindungen (WLAN) und Hotspots

Drahtlose Verbindungen werden auch im betrieblichen Umfeld immer populärer. Die meisten neuen Notebooks sind bereits mit WLAN-Adaptoren ausgestattet, und auch Desktop-PCs lassen sich mit einer WLAN-Einsteckkarte schnell und einfach so mobil machen, dass sie innerhalb des Firmengebäudes an beliebigen Plätzen eingesetzt werden können. Doch der Komfort hat seinen Preis: Drahtlose Verbindungen können sehr leicht abgehört werden und öffnen das System für potenzielle Eindringlinge. WLAN-Verbindungen aller Art - insbesondere auch Verbindungen zu öffentlichen Hotspots - müssen besonders sorgfältig geschützt werden. Dabei ist immer zu bedenken, dass die Angriffe aus sicherer Entfernung stattfinden, da die Funkwellen weder an Zimmer- noch an Grundstücksgrenzen Halt machen.

Checkliste 8: Software-Nutzung und Software-Updates

Der Umgang mit Software und vor allem mit Software-Updates ist auch ein äußerst wichtiges Sicherheitsthema. Ständige softwaretechnische Neuerungen und die Entdeckung immer neuer Sicherheitslücken machen es erforderlich, dass Anwendungsprogramme und Betriebssysteme immer wieder auf den neuesten Stand gebracht werden. Solange die Updates von zentral Verantwortlichen durchgeführt werden, klappt dies meistens gut. Anders ist es, wenn die Durchführung der Updates in den Händen der einzelnen Mitarbeiter liegt. Da diese die ständigen Update-Aufforderungen sehr schnell leid sind, werden Updates häufig nur noch sporadisch durchgeführt. Wie fatal dies sein kann, zeigt sich daran, dass fast alle Schäden, die durch aktuelle Würmer und Viren verursacht wurden, komplett hätten vermieden werden können, wenn nur die bereits vorliegenden Windows-Updates durchgeführt worden wären. Software, die unkontrolliert aus dem Internet heruntergeladen oder von zu Hause mitgebracht

und auf betrieblichen PCs eingesetzt wird, stellt ebenfalls ein erhebliches Risiko dar, das es durch verbindliche Vereinbarungen einzudämmen gilt.

Checkliste 9: Schutzvorkehrungen und Schutzeinrichtungen

Dieser Sicherheitsbereich beschäftigt sich mit den Schutzmaßnahmen, die nur indirekt mit dem Computersystem und anderen vorhandenen IT-Einrichtungen zu tun haben. Dabei spielen auch Zugangskontrollen eine wichtige Rolle: Die Sicherheitsmaßnahmen, die gegen unbefugte Zugriffe auf das Computersystem über das Internet getroffen wurden, können ja höchst wirksam sein. Wenn aber jemand völlig unbemerkt und unbehelligt in ein Büro spazieren und einen kompletten Rechner entwenden kann, auf dem sich sicherheitsrelevante Daten befinden, nützt natürlich auch die beste Firewall nichts.

Checkliste 1: Sicherheitsmanagement

Leitfrage	Ja	Nein	Prüfen
Hat die Unternehmensleitung verbindliche IT-Sicherheitsziele festgelegt und die eigene Verantwortung der Geschäftsführung für die IT-Sicherheit ebenfalls ausdrücklich schriftlich fixiert?	☐	☐	☐
Gibt es einen IT-Sicherheitsbeauftragten?	☐	☐	☐
Wurde der IT-Sicherheitsbeauftragte angemessen geschult?	☐	☐	☐
Muss ein Datenschutzbeauftragter gestellt werden?	☐	☐	☐
Werden IT-Sicherheitserfordernisse bei neuen Projekten, insbesondere bei der Planung von Netzwerkerweiterungen, Neuanschaffungen von Computer- und Kommunikationssystemen und IT-Dienstleistungsverträgen, frühzeitig berücksichtigt?	☐	☐	☐
Gibt es eine Planung für die Umsetzung der Sicherheitsziele und der erforderlichen IT-Sicherheitsmaßnahmen?	☐	☐	☐
Werden bei der Planung und Umsetzung der Sicherheitsmaßnahmen alle erforderlichen gesetzlichen Rahmenbedingungen beachtet?	☐	☐	☐
Wird der Datenschutzbeauftragte in die Entscheidungsprozesse für die Festlegung der Sicherheitsmaßnahmen eingebunden?	☐	☐	☐
Ist in der Planung berücksichtigt worden, ob die Sicherheitsmaßnahmen einmalig oder regelmäßig durchgeführt werden müssen?	☐	☐	☐
Gibt es einen Terminplan für die Überprüfung der Sicherheitsmaßnahmen?	☐	☐	☐
Gibt es eine Liste, in der die Zuständigkeiten und Verantwortlichkeiten für die Umsetzung der IT-Sicherheitsmaßnahmen festgelegt sind?	☐	☐	☐
Sind die notwendigen Passwörter so hinterlegt, dass notfalls auch andere Mitarbeiter die Sicherheitsmaßnahmen durchführen können?	☐	☐	☐
Sind die bestehenden Sicherheitsrichtlinien und Zuständigkeiten allen Mitarbeitern bekannt, die mit der Durchführung von Sicherheitsmaßnahmen betraut sind?	☐	☐	☐
Gibt es Checklisten, in denen genau aufgeführt ist, was in Bezug auf die IT-Sicherheit beim Eintritt neuer Mitarbeiter und beim Ausscheiden von Mitarbeitern zu beachten ist (Kennwörter, Berechtigungen, Schlüssel, Security-Card usw.)?	☐	☐	☐

Wird die Wirksamkeit der IT-Sicherheitsmaßnahmen regelmäßig überprüft?	☐	☐	☐
Ist das IT-Sicherheitskonzept dokumentiert und steht es allen Mitarbeitern zur Verfügung?	☐	☐	☐
Gibt es IT-Sicherheitsrichtlinien, die jedem Mitarbeiter ausgehändigt werden?	☐	☐	☐

Checkliste 2: Allgemeine Sicherheitsaspekte und Verhalten in Notfällen

Leitfrage	Ja	Nein	Prüfen
Viele Programme und EDV-Anwendungen sind bereits mit bestimmten Schutzmechanismen ausgestattet. Werden diese Schutzmechanismen genutzt?	☐	☐	☐
Werden Virenschutzprogramme flächendeckend eingesetzt und ständig aktualisiert?	☐	☐	☐
Sind Firewall-Lösungen vorhanden und werden diese eingesetzt?	☐	☐	☐
Sind allen Benutzern des Computersystems Benutzernamen, Kennwörter und bestimmte Rechte bzw. Rollen und Profile zugeteilt worden?	☐	☐	☐
Gibt es Zugriffsbeschränkungen und ist klar geregelt, auf welche Daten jeder Mitarbeiter zugreifen darf?	☐	☐	☐
Gibt es auch für Administratoren unterschiedliche Zugriffsrechte und/oder unterschiedliche Rollen und Profile?	☐	☐	☐
Ist geregelt, welche Rechte und Privilegien Anwenderprogramme und Benutzer innerhalb des Computersystems haben?	☐	☐	☐
Werden bei IT-Komponenten die werkseitigen Standardeinstellungen für Benutzernamen und Kennwörter geändert und angepasst?	☐	☐	☐
Werden sicherheitsrelevante Programme und Funktionen, die nicht benötigt werden, tatsächlich deinstalliert und deaktiviert?	☐	☐	☐
Wissen alle Benutzer, wie sie sicherheitskonform handeln und Risiken beim Internetzugriff sowie beim Empfangen und Versenden von E-Mails vermeiden?	☐	☐	☐
Wissen alle Benutzer, wie sie sich verhalten sollten, wenn ein Virenschutzprogramm einen Schadprogrammbefall meldet?	☐	☐	☐
Gibt es aktuelle schriftliche Handlungsanweisungen für die sicherheitskonforme Computernutzung?	☐	☐	☐
Werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?	☐	☐	☐
Gibt es einen Notfallplan für alle wichtigen Notfallsituationen, der außer detaillierten Verhaltensanweisungen auch Namen und Kontaktangaben von Verantwortlichen und Ansprechpartnern enthält?	☐	☐	☐
Werden die angegebenen Handlungsanweisungen und Kontaktadressen regelmäßig überprüft und aktualisiert?	☐	☐	☐

Wissen alle Mitarbeiter, dass es einen Notfallplan gibt, und wie dieser zugänglich ist?	☐	☐	☐
---	--------------------------	--------------------------	--------------------------

Checkliste 3: Sicherheitsbewusstsein

Leitfrage	Ja	Nein	Prüfen
Werden die Mitarbeiter regelmäßig in sicherheitsrelevanten Themen geschult?	☐	☐	☐
Werden vertrauliche Informationen und Datenträger mit vertraulichen Informationen sorgfältig aufbewahrt und zusätzlich geschützt?	☐	☐	☐
Erhalten alle Mitarbeiter einen Sicherheitsleitfaden, in dem sämtliche sicherheitsrelevanten Themen und ein Verhaltenskodex enthalten sind?	☐	☐	☐
Sind alle Mitarbeiter mit den Grundsätzen des rechtskonformen Umgangs mit personenbezogenen Daten vertraut?	☐	☐	☐
Werden vertrauliche Informationen vor Wartungs- und Reparaturarbeiten von Datenträgern und IT-Systemen, die Mitarbeitern von Fremdfirmen zugänglich sein könnten, entfernt und gelöscht?	☐	☐	☐
Gibt es Maßnahmen, die das Sicherheitsbewusstsein der Mitarbeiter erhöhen sollen?	☐	☐	☐
Werden die bestehenden Sicherheitsvorgaben kontrolliert und Verstöße dagegen geahndet?	☐	☐	☐

Checkliste 4: Benutzernamen, Kennwörter und Verschlüsselung

Leitfrage	Ja	Nein	Prüfen
Werden die Sicherheitsmechanismen der eingesetzten Programme genutzt und sind Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung vorhanden und aktiviert?	☐	☐	☐
Ist sichergestellt, dass voreingestellte oder leere Pass- und Kennwörter geändert wurden?	☐	☐	☐
Gibt es Vergaberichtlinien für Benutzernamen sowie Pass- und Kennwörter?	☐	☐	☐
Werden Benutzernamen und Pass- und Kennwörter zentral dokumentiert?	☐	☐	☐
Wenn Mitarbeiter selbst Pass- und Kennwörter vergeben: Sind alle Mitarbeiter in der Vergabe sicherer Kennwörter geschult und werden auch die selbst vergebenen Kennwörter zentral dokumentiert?	☐	☐	☐
Werden Arbeitsplatzrechner mit Bildschirmschoner und dazugehörigem Kennwort gesichert und vor neugierigen Blicken geschützt?	☐	☐	☐
Werden vertrauliche Daten und besonders gefährdete Systeme (z. B. Notebooks und andere mobile Informationssysteme) durch Verschlüsselung geschützt?	☐	☐	☐
Ist gewährleistet, dass vertrauliche Daten per E-Mail verschlüsselt	☐	☐	☐

übertragen werden?			
Werden Computer, auf denen sich sicherheitsrelevante Daten befinden, durch zusätzliche Sicherheitsmaßnahmen (z. B. durch Security Cards oder externe Authentifizierung) geschützt?	☐	☐	☐
Erfolgt der externe Zugriff auf das lokale Firmennetzwerk über getunnelte und durch Verschlüsselung gesicherte VPN-Verbindungen?	☐	☐	☐

Checkliste 5: Internet und E-Mail

Leitfrage	Ja	Nein	Prüfen
Gibt es eine Firewall?	☐	☐	☐
Wird die Konfiguration der Firewall regelmäßig kontrolliert und aktualisiert?	☐	☐	☐
Ist festgelegt, welche Daten übers Internet angeboten/verschickt werden dürfen?	☐	☐	☐
Ist festgelegt, wie mit sicherheitsgefährdenden Zusatzprogrammen (PlugIns) und aktiven Inhalten (z. B. ActiveX) umgegangen wird?	☐	☐	☐
Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?	☐	☐	☐
Sind Web-Browser und E-Mail-Programme sicher konfiguriert?	☐	☐	☐
Sind die Mitarbeiter ausreichend für die Internetnutzung und den E-Mail-Einsatz geschult?	☐	☐	☐
Gibt es verbindliche Richtlinien für die Nutzung des Internets?	☐	☐	☐
Gibt es eine E-Mail-Sicherheitsrichtlinie?	☐	☐	☐
Gibt es Vorkehrungen gegen Spam-Mails (z. B. Filter)?	☐	☐	☐
Wissen alle Benutzer, wie sie mit den Spam-Mails, die trotz der Spam-Filter in den Posteingang gelangen, umgehen sollen?	☐	☐	☐
Sind alle Mitarbeiter über Phishing-Attacken informiert und wissen sie, wie sie sich in Bezug auf Phishing-Mails zu verhalten haben?	☐	☐	☐
Gibt es eine Regelung für privates Surfen und private E-Mail-Korrespondenz?	☐	☐	☐

Checkliste 6: Datensicherung

Leitfragen	Ja	Nein	Prüfen
Gibt es einen Plan für die zentrale Datensicherung?	☐	☐	☐
Gibt es feste Verantwortlichkeiten für die Durchführung der zentralen Datensicherung?	☐	☐	☐
Ist festgelegt, welche Daten wie lange gesichert werden?	☐	☐	☐
Ist berücksichtigt, dass die Daten in mehreren Sicherungssätzen gesichert und ältere Sicherungen mit neueren Sicherungen überschrieben werden?	☐	☐	☐

Werden die Sicherungssätze an unterschiedlichen Orten innerhalb und außerhalb des Unternehmens verteilt aufbewahrt?	☐	☐	☐
Erfolgt eine externe Sicherung der Daten über eine sichere Internetverbindung?	☐	☐	☐
Werden wichtige Daten täglich gesichert?	☐	☐	☐
Ist eine schnelle Rücksicherung der Daten möglich?	☐	☐	☐
Werden die Sicherungsdatenträger regelmäßig kontrolliert?	☐	☐	☐
Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?	☐	☐	☐
Sind die Mitarbeiter verpflichtet, regelmäßig Sicherungen ihrer eigenen Dokumente vorzunehmen, und sind sie mit der Wiederherstellung der Daten vertraut?	☐	☐	☐

Checkliste 7: Drahtlose Netzwerkverbindungen (WLAN) und Hotspots

Leitfragen	Ja	Nein	Prüfen
Ist die Außenreichweite der WLAN-Access-Points bekannt?	☐	☐	☐
Wurden bei WLAN-Access-Points und WLAN-Routern die werkseitig eingestellten Kennwörter geändert?	☐	☐	☐
Sind die WLAN-Verbindungen mit einem speziellen Netzwerkkennwort (SSID) gesichert?	☐	☐	☐
Ist auf den WLAN-Komponenten die WPA2-Verschlüsselung aktiviert?	☐	☐	☐
Sind auf den WLAN-Access-Points und -Routern die MAC-Adressen der zugelassenen WLAN-Adapter eingetragen?	☐	☐	☐
Sind zusätzliche Authentifizierungsmechanismen aktiviert?	☐	☐	☐

Checkliste 8: Software-Nutzung und Software-Updates

Leitfrage	Ja	Nein	Prüfen
Gibt es einen Verantwortlichen für Sicherheits-Updates?	☐	☐	☐
Werden Sicherheits-Updates regelmäßig eingespielt?	☐	☐	☐
Werden Windows-Updates zentral vorgenommen?	☐	☐	☐
Werden die neuen Sicherheitseinrichtungen von Windows Vista in vollem Umfang genutzt?	☐	☐	☐
Sind Benutzer verpflichtet, Sicherheits- und Windows-Updates selbst durchzuführen?	☐	☐	☐
Wird die Durchführung der Software-Updates regelmäßig überprüft?	☐	☐	☐
Werden Updates für Anwendungsprogramme getestet, bevor sie für die allgemeine Verwendung freigegeben werden?	☐	☐	☐
Wurden alle Benutzer darauf hingewiesen, dass Programme aus dem Internet nur nach ausdrücklicher Genehmigung des Systemverwalters	☐	☐	☐

heruntergeladen und installiert werden dürfen?			
Ist es den Benutzern ausdrücklich untersagt worden, eigene Programme auf den Firmen-PCs zu installieren?	☐	☐	☐

Checkliste 9: Schutzvorkehrungen und Schutzeinrichtungen

Leitfrage	Ja	Nein	Prüfen
Sind die Server des Computersystems ausreichend gegen Feuer, Überhitzung und Wasserschäden geschützt?	☐	☐	☐
Sind die Server und wichtige Arbeitsplatzrechner gegen Überspannungen und Stromausfall geschützt?	☐	☐	☐
Ist der Zutritt zu wichtigen Teilen des Computersystems und den Serverräumen geregelt?	☐	☐	☐
Gibt es eine Eingangskontrolle?	☐	☐	☐
Müssen Besucher, Handwerker und andere externe Dienstleister beaufsichtigt werden?	☐	☐	☐
Gibt es Überwachungskameras?	☐	☐	☐
Ist das Firmengelände gegen unbefugtes Betreten gesichert?	☐	☐	☐
Besteht ein ausreichender Schutz vor Einbrechern?	☐	☐	☐
Werden Firmengelände und Firmengebäude nachts von einem Wachdienst kontrolliert?	☐	☐	☐
Ist der Bestand von Hard- und Software in einer Inventarliste erfasst und werden regelmäßige Bestandskontrollen durchgeführt?	☐	☐	☐
Sind wichtige Geräte durch zusätzliche Maßnahmen (z. B. Magnetstreifen) geschützt, die einen Sicherheitsalarm auslösen, wenn diese unbefugt entfernt werden?	☐	☐	☐