

IT-Security-Checkliste

Version: 3.0 vom 14.11.05 / Rolf Kessler HKC und Beat Burkart HKC

Dieses Dokument ist zur Überprüfung Ihrer IT gedacht, und zwar durch Sie selbst oder einen Ihrer Mitarbeiter. Das Dokument ist nur als Hilfsmittel und Reminder gedacht, Ihre eigenen Bedürfnisse können in einzelnen Punkten stark von den hier dargestellten abweichen.

Dieses Dokument ist bewusst in einer Sprache abgefasst, die auch ein Nicht-IT-Spezialist verstehen sollte, ein gewisses technisches Verständnis wird aber vorausgesetzt. Einige Fachbegriffe mussten bei der Abfassung des Dokumentes dennoch verwendet werden.

Eine Mehrzahl der Angriffe geschieht von internen Quellen. Diese Problematik muss oft organisatorisch gelöst werden. Viele der in diesem Punkt beschriebenen Punkte sind technisch und damit auch vor allem für Angriffe von aussen gedacht.

Grundlagen

Allgemeines

Nr.	Beschreibung	Ja	Nein	Weiss nicht
1	Bin ich mit dem Schweizer Datenschutzgesetz einigermaßen vertraut? www.admin.ch/ch/d/sr/c235_1.html	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Bin ich mit dem IT-Grundschutzhandbuch vertraut? www.bsi.de/gshb/	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Business-Continuity-Plan

Nr.	Beschreibung	Ja	Nein	Weiss nicht
3	Bin ich mir bewusst, wie lange ich bei einem Ausfall der IT-Systeme den Betrieb weiterführen kann?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Gibt es ein schriftliches Papier über die Massnahmen, die beim Ausfall der Systeme getroffen werden müssen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Risikobeurteilung, Schutzziel und Massnahmen

Nr.	Beschreibung	Ja	Nein	Weiss nicht
5	Habe ich eine Risikomatrix für meine Systeme erstellt? (Gegenüberstellung von Wahrscheinlichkeit eines Ausfalles / Schadenausmass).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Habe ich anschliessend Massnahmen zur Risikominderung inklusive Kostenanalyse eruiert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	Bin ich mir über die geforderte Verfügbarkeit der einzelnen System im Klaren?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Systeme und Software

Allgemeines

Nr.	Beschreibung	Ja	Nein	Weiss nicht
1	Habe ich ein Patch-Management für meine PC und Server etabliert? (Beispielsweise ein Microsoft WSUS-Service)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Sind die Server in einem abgeschlossenen Serverraum oder wenigstens ein abgeschlossener Serverschrank aufbewahrt? (Wenn ein Spezialist physikalischen Zugriff auf eine Maschine hat, dauert es im Normalfalle keine fünf Minuten um beispielsweise das Administrator-Passwort neu zu setzen).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Sind meine kritischen Hardware-Systeme unter einem Wartungsvertrag mit definierten Reaktionszeiten bei einem Lieferanten? (Bsp. ein HP Care Pack) Achtung: Nicht nur Server können kritisch sein, sondern auch beispielsweise ADSL-Router, ja sogar dedizierte PC (z.B. Kesselsteuerung in einem Pharmabetrieb).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Server

Nr.	Beschreibung	Ja	Nein	Weiss nicht
4	Gibt es in meinem Betrieb Richtlinien zum Einsatz von Passwörtern oder überlasse ich das jedem einzelnen Mitarbeiter?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Sind die Daten der Mitarbeiter in dedizierten Bereichen (Dateifreigabe) auf dem Server gespeichert wo Sie auch zentral gesichert werden können?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Datensicherung, Datenwiederherstellung

Nr.	Beschreibung	Ja	Nein	Weiss nicht
6	Gibt es bei mir eine regelmässige (tägliche) Datensicherung?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	Wird auch periodisch (z.B. monatlich) versucht, ob Daten ab Band wiederhergestellt werden können?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	Wird periodisch (z.B. wöchentlich) ein Band off-site gelagert? Dies ist wichtig für einen Katastrophenfall wie Brand oder Hochwasser. Achtung: In feuersicheren Safes werden die Bänder schon nach ca. 1 Stunde Brand entmagnetisiert und können danach nicht mehr gelesen werden.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	Sind meine Bänder weggeschlossen? (Auf einem Band sind Ihre Firmendaten gespeichert, jeder IT Spezialist kann diese Bänder wieder einlesen!)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	Werden meine Tagesbänder periodisch (z.B. halb-jährlich) ausgewechselt? Bänder werden mit der Zeit schlecht, besonders DAT-Bänder sind anfällig.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	Gibt es eine Protokollierung, wann welches Band eingelegt werden muss?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	Überprüft jemand den Backup, ob er erfolgreich verlaufen ist?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Client (Notebook und Desktop)

Nr.	Beschreibung	Ja	Nein	Weiss nicht
13	Wird für Benutzer die viel unterwegs sind eine Software-Firewall eingesetzt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	Werden die lokalen Daten von Notebook-Benutzern auch gesichert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	Ist die Hard-Disk von Notebook Benutzern verschlüsselt? (Diebstahl- oder Verlust des Notebook)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	Ist die Verwendung von USB (Memory-Sticks) und Disketten geregelt oder sogar unterbunden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17	Wird die Antivirussoftware und die Antispywaresoftware auf Notebooks auch periodisch aktualisiert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Netzwerk

Nr.	Beschreibung	Ja	Nein	Weiss nicht
18	Gibt es ein Plan meines Netzwerkes?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19	Ist mein Netzwerk inventarisiert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20	Verlaufen Netzkabel durch öffentliches Gebiet (z.B. Garagen). Wenn ja, macht es Sinn über verschlüsselten Datenverkehr nachzudenken, dieser kann bei Microsoft Systemen relativ einfach vom Spezialisten konfiguriert werden.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21	Ist der Zugriff auf mein Netzwerk eingeschränkt auf bekannte PC. (Man kann z.B. die Hardware-Adresse der Netzkarte in viele Netzwerkgeräte einprogrammieren.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22	Sind die nicht verwendeten Netzwerkdienste auf den einzelnen PC deaktiviert? Standardmässig sind viele Dienste aktiv, die gar nicht benötigt werden, aber allenfalls ein grosses Angriffspotenzial für Hacker haben. So zum Beispiel der standardmässig installierte Internet Information Server auf einem Windows 2000 Server.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23	Gibt es DNS (Domain-Name Server) Einträge die vom Internet her sichtbar sind und nicht benötigt werden? Falls nötig, von einem Spezialisten überprüfen lassen.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
24	Wird mein Netzwerk gegen aussen (das Internet) mit einer Hardware-Firewall abgeschottet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
25	Ist diese Firewall von einem internen oder externen Spezialisten überprüft und konfiguriert worden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Virenschutz, Antispyware Spamfilter

Nr.	Beschreibung	Ja	Nein	Weiss nicht
26	Setze ich eine Anti-Virus-Software auf den Servern und den PC ein?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27	Sind die Antivirussignaturen aktuell? Die Hersteller liefern in der Zwischenzeit fast täglich neue Signaturen aus.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
28	Gibt es eine Anti-Virus-Software auf dem Mail-Server oder meinem Provider? Sind deren Signaturen aktuell? Im Viren-Bereich stellt das Mail-System mit Abstand die grösste Gefahr dar.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
29	Haben meine Benutzer Erfahrung im Umgang mit Mails (speziell mit Attachments) von unbekanntem Absendern?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
30	Benutzen wir einen Antispywareschutz? Achtung: Die Gefahr von Spyware wird von vielen Leuten schon grösser als die von Viren eingeschätzt, einfacher Grund: Spyware ist kommerziell, da steckt viel Geld dahinter.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
31	Wird der Antispywareschutz automatisch aktualisiert und ist er aktuell?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
32	Wird bei uns ein Spamfilter eingesetzt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
33	Wird bei uns ein Internet-Download-Schutz eingesetzt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>