Cyber-Sicherheits-Check für Ihr Unternehmen

Karsten Thomas
Manager IT Audit & Advisory

Certified Cyber Security Practitioner
Certified Information Systems Auditor
Certified in Risk and Information Systems Control

INHALT

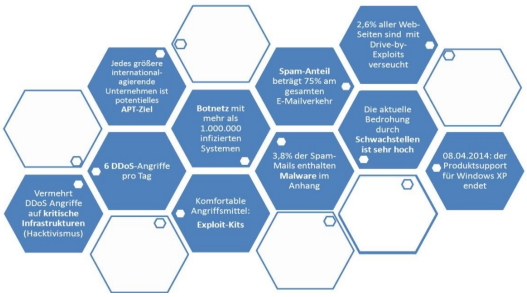
Cyber-Sicherheits-Check

Heute ist es erforderlich, den Bereich der klassischen IT-Sicherheit auf den gesamten „Cyber-Raum“ zu erweitern. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik sowie darauf basierende Anwendungen, Prozesse, verarbeitete Informationen und Kommunikation. Somit beinhaltet der Cyber-Raum nahezu die gesamte moderne Informations- und Kommunikationstechnik.

Mit dem Cyber-Sicherheits-Check bieten wir Ihnen eine effiziente Möglichkeit, diesen Bereich in Ihrem Unternehmen zu beurteilen, damit Sie Verbesserungsbedarf erkennen und einen angemessenen Schutz aufbauen können.

Cyber-Sicherheit im Unternehmen

Unternehmen sind bei den Geschäftsprozessen und Arbeitsabläufen in der Regel auf eine verlässliche und fehlerfrei funktionierende IT-Landschaft angewiesen. Ein Ausfall der IT stellt daher ebenso wie ein unkontrollierter Zugriff oder die Manipulation von Daten ein operationelles Risiko dar. Gegen Ausfälle wird meist eine Vorsorge getroffen, Risiken durch Angriffe von außen werden dabei jedoch häufig vernachlässigt.



© BSI

Cyber-Angriffe auf Unternehmen sind nicht nur Großkonzernen vorbehalten. Das laufende Monitoring des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zeigt, dass auch kleinere mittelständische Unternehmen aller Branchen im Fokus von Angriffen stehen. Dabei kann es sich um ungezielte Attacken handeln, die von Bot-Netzen ausgehend automatisiert Sicherheitslücken in nicht angemessen geschützten Netzwerken ausnutzen, aber auch zunehmend um gezielte Angriffe, um an Daten Ihres Unternehmens zu gelangen oder einen finanziellen Schaden zu verursachen. In der Regel sind mit den Angriffen finanzielle Interessen, Sabotageabsichten, Informationsbeschaffung oder politische Interessen verbunden.

Je nach Branche sind Daten der Forschung und Entwicklung, aber auch Kundendaten, Bankdaten, Quellcodes etc. das Ziel der Angreifer. Der Schaden für das Unternehmen ergibt sich beispielsweise aus dem (oft unbemerkten) Verlust von Daten, aus finanziellen Nachteilen, aber auch Systemausfällen oder unbemerkt veränderten Informationen. Im Unterschied zu den nichtvirtuellen Bedrohungen besteht die Gefahr von Cyber-Angriffen auch darin, dass sie in vielen Fällen unentdeckt bleiben und der Schaden bei Entdeckung mitunter weitaus größer ist.

Nach Informationen des BSI besitzen derzeit die folgenden Gefährdungen eine besonders hohe Relevanz:

- gezieltes Hacking von Webservern,
- Infiltration von Rechnern beim Internetzugriff durch Mitarbeiter,
- gezielte Infiltration über E-Mail-Anhänge,
- Denial-of-Service-Attacken,
- ungezielte Verteilung von Schadsoftware z.B. durch SPAM-Mails sowie
- mehrstufige Angriffe.

Was ist der Cyber-Sicherheits-Check?

MAZARS ist Mitglied der Allianz für Cyber-Sicherheit, einer Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet wurde. Als Zusammenschluss der wichtigen deutschen IT-Sicherheitsorganisationen und einer Vielzahl von namhaften Unternehmen hat die Allianz das Ziel, aktuelle und valide Informationen zur IT-Sicherheit flächendeckend und aus erster Hand bereitzustellen.

Der Cyber-Sicherheits-Check wurde im Rahmen dieser Initiative vom ISACA Germany Chapter e.V. gemeinsam mit Experten des BSI entwickelt und bietet mit einem strukturierten Leitfaden ein einheitliches Vorgehen für die Beurteilung der Cyber-Sicherheit im Unternehmen. So ist sichergestellt, dass die Ergebnisse dieser Beurteilung eine hohe Qualität und Aussagekraft besitzen.

Bei dem Cyber-Sicherheits-Check handelt es sich um eine Aufnahme und Beurteilung der Maßnahmen zur Informationssicherheit in Bezug auf den Cyber-Raum, d.h. die Bereiche, die mit der aktiven und passiven Nutzung des Internets zusammenhängen (Netzwerk, Firewall, VPN-Zugänge, mobile Endgeräte, Webserver, eMail-Nutzung, Webshop, Anbindung an andere Netze usw.). Wir bestimmen anhand des Leitfadens das aktuelle Niveau der Cybersicherheit in Ihrem Unternehmen. Das Ergebnis des Cyber-Sicherheits-Checks bietet Ihnen die Möglichkeit einer Risikoeinschätzung und der Planung des weiteren Vorgehens zur Einleitung entsprechender Folgemaßnahmen.

Cyber-Sicherheits-Check für Ihr Unternehmen

Als Mitglied der Allianz für Cyber-Sicherheit und mit zertifizierten Beratern bieten wir Ihnen mit dem Cyber-Sicherheits-Check eine Beurteilung der Informationssicherheit / Cyber-Sicherheit in Ihrem Unternehmen an. Wir sind davon überzeugt, dass die effiziente Bewertung auch Ihrem Unternehmen helfen kann, die Informationssicherheitsmaßnahmen mit Bezug zur Nutzung des Internets nachhaltig zu verbessern. Dies ist im Vergleich zu anderen Methoden mit dem Cyber-Sicherheits-Check schon in sehr kurzer Zeit möglich.

Der große Vorteil des Cyber-Sicherheits-Checks im Vergleich zu weiteren Methoden wie z.B. BSI-Grundschutz oder ISO 27001 liegt darin, dass diese Beurteilung sehr flexibel an Ihr Unternehmen und den Schutzbedarf angepasst werden kann. Grundsätzlich werden alle Bereiche Ihres Unternehmens betrachtet, eine Priorisierung der Themen ergibt sich aus der individuellen Gefährdungslage und dem Schutzbedarf Ihres Unternehmens.

Somit ist der Cyber-Sicherheits-Check im Gegensatz zu aufwändigen mehrwöchigen Prüfungen in Form eines Quick-Checks durchführbar und berücksichtigt dennoch risikoorientiert die wesentlichen Bereiche. So erhalten

Sie mit einem externen Aufwand von wenigen Tagen und einem vergleichsweise geringen internen Aufwand einen guten Überblick über Ihre Sicherheitsmaßnahmen. Der Cyber-Sicherheits-Check basiert fachlich auf den Inhalten von BSI-Grundschutz, ISO 27001, COBIT und PCI-DSS. Damit bildet er keine weitere Alternative zu diesen Standards, sondern ist damit kompatibel, ist parallel zur Anwendung dieser Grundlagen durchführbar und erlaubt eine direkte Zuordnung der betrachteten Inhalte zu eventuell bereits vorhandenen Aktivitäten in diesem Umfeld.

Unsere Vorgehensweise

Der standardisierte Cyber-Sicherheits-Check besteht aus den folgenden Teilschritten:

- Bestimmung der Cyber-Sicherheits-Exposition in Ihrem Unternehmen (Einschätzung der realen „Betroffenheit“ und des Schutzbedarfs),
- Sichtung vorhandener Dokumente,
- Vorbereitung der Vor-Ort-Beurteilung einschließlich Planung der zu betrachtenden Inhalte,
- Vor-Ort-Beurteilung mit Abschlussgespräch und
- Nachbereitung / Berichterstellung.

Die Vor-Ort-Beurteilung nimmt dabei meist einen Zeitraum zwischen einem und drei Tagen in Anspruch.

Keine Risiken

Da der Cyber-Sicherheits-Check ohne aktive Eingriffe in die IT-Systeme durchgeführt wird, ergeben sich während der Durchführung keine Risiken durch die Prüfung selbst. Es erfolgt kein eigenständiger unbegleiteter Zugriff auf Ihre Systeme, sondern der Check erfolgt anhand von

- Interviews,
- Prüfungen von Konfigurationseinstellungen,
- Beobachtungen am geprüften Standort,
- Aktenanalyse,
- Datenanalysen z.B. bei Logfiles sowie
- ggf. schriftlichen Befragungen.

Da der Cyber-Sicherheits-Check fachlich auf den Inhalten von BSI-Grundschutz, ISO 27001, COBIT und PCI-DSS basiert und verschiedene Bereiche Ihres Unternehmens betrachtet, setzt die Durchführung eine hohe Erfahrung des Prüfers in diesen Bereichen voraus. Daher setzen wir ausschließlich erfahrene Mitarbeiter ein, welche über eine entsprechende Qualifikation als Certified Information Systems Auditor (CISA) oder ISO 27001 Lead Auditor verfügen.

Ergebnis des Cyber-Sicherheits-Checks

Im Ablauf des Cyber-Sicherheits-Checks werden Schwachstellen identifiziert, welche in Sicherheitsempfehlungen, Sicherheitsmängeln oder schwerwiegenden Sicherheitsmängeln münden. Die Einschätzung erfolgt dabei durch den Prüfer. Gleichzeitig empfehlen wir Ihnen mögliche Maßnahmen basierend auf den im Leitfaden Cyber-Sicherheits-Check definierten Maßnahmenzielen. Im Anschluss können wir Sie bei der Umsetzung von entsprechenden Gegenmaßnahmen unterstützen und helfen Ihnen, die Informationssicherheit in Ihrem Unternehmen nachhaltig zu verbessern.

- Sie erhalten einen Überblick über den Stand der Cyber-Sicherheit in Ihrem Unternehmen,
- Sie kennen die Schwachstellen und können diese bewerten,
- Sie können erste Schutzmaßnahmen definieren und umsetzen,
- Sie erhalten eine auf Ihr Unternehmen zugeschnittene Risikoeinschätzung und
- Sie wissen, an welchen Stellen Sie sich vor Wirtschaftsspionage schützen müssen.

Warum Mazars?

Wir verfügen über eine langjährige und breite Expertise in IT-Sicherheit und -Prüfung in verschiedenen Branchen, u.a. Industrie, Handel, Dienstleistungen, Finanzdienstleistungen, Banken und öffentliche Organisationen, und zu unterschiedlichen IT-Systemen und -Landschaften.

Aufgrund unserer internationalen Präsenz können wir Sie an sämtlichen Standorten im In- und Ausland professionell begleiten. Unsere gute internationale Zusammenarbeit wird durch unsere Competence-Center zur IT-Sicherheit unterstützt.

Wir berücksichtigen Standards und Best-Practice-Modelle und gewährleisten eine hohe Prüfungseffizienz und Prüfungssicherheit durch MAZARS-Vorgehensmodelle, die im Rahmen des Projektes auf die kundenindividuellen Anforderungen angepasst werden.

Wir schauen über den Tellerrand aufgrund unserer Erfahrungen aus verschiedenen Audits (projektbegleitende IT-Prüfungen, Zertifizierung von Serviceprovidern, Softwareprüfungen, Migrationsprüfungen, Jahresabschlussprüfungen, Sonderprüfungen, Prüfungen des internen Kontrollsystems etc.).

Wir bieten die hohe Qualität und Zuverlässigkeit einer großen Wirtschaftsprüfungsgesellschaft und können Sie mit unserer Expertise auch bei weiteren Maßnahmen zur IT-Sicherheit unterstützen.

Gerne stehen wir Ihnen zu diesem Thema zur Verfügung - sprechen Sie uns an.

Karsten Thomas
Manager IT Audit & Advisory

MAZARS GmbH Wirtschaftsprüfungsgesellschaft
Bennigsen-Platz 1
40474 Düsseldorf

Telefon: +49 211 8399 431
Mobil: +49 177 711 5599
E-Mail: karsten.thomas@mazars.de

MAZARS ist eine internationale integrierte Wirtschaftsprüfungs- und Beratungsgesellschaft europäischen Ursprungs. Die Gesellschaft ist mit 13.800 Mitarbeitern in 72 Ländern weltweit vertreten. In Deutschland betreut MAZARS mit 300 Mitarbeitern an sechs Standorten.

BERLIN
Hausvogteiplatz 10
10117 Berlin
Telefon: +49 30 200774-0
Fax: +49 30 200774-44
E-Mail: berlin@mazars.de

DÜSSELDORF
Bennigsen-Platz 1
40474 Düsseldorf
Telefon: +49 211 8399-0
Fax: +49 211 8399-133
E-Mail: duesseldorf@mazars.de

FRANKFURT
Theodor-Stern-Kai 1
60596 Frankfurt
Telefon: +49 69 96765-0
Fax: +49 69 96765-2160
E-Mail: frankfurt@mazars.de

LEIPZIG
Riemannstraße 29b
04109 Leipzig
Telefon: +49 341 1263-0
Fax: +49 341 1263-133
E-Mail: leipzig@mazars.de

MÜNCHEN
Bernhard-Wicki-Straße 7
80636 München
Telefon: +49 89 21636-0
Fax: +49 89 21636-133
E-Mail: muenchen@mazars.de

STUTTGART
Friedrichstraße 10
70174 Stuttgart
Telefon: +49 711 601787-0
Fax: +49 711 601787-17
E-Mail: stuttgart@mazars.de

MAZARS