Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: IT IM UNTERNEHMEN

Basismaßnahmen der Cyber-Sicherheit

Die Absicherung von Netzen und IT-Systemen in Unternehmen, Behörden und anderen Organisationen stellt angesichts der hochdynamischen Entwicklung der Bedrohungslage im Cyber-Raum eine komplexe und immer wieder neu herausfordernde Aufgabe dar.

Um den zahlreichen aus Perspektive der Cyber-Sicherheit entstehenden Anforderungen gerecht zu werden, bieten nationale und internationale Standards, Leitfäden und Handlungsempfehlungen den Verantwortlichen für IT-Planung und -Betrieb mögliche Vorgehensweisen an. Autoren und Herausgeber sind dabei sowohl staatliche Stellen, Hersteller und Sicherheitsdienstleister als auch die akademische Forschung.

Eine Herausforderung besteht jedoch darin, aus der Vielzahl verfügbarer Quellen die entscheidenden Antworten auf Schlüsselfragen der Cyber-Sicherheit zu identifizieren und daraus abgeleitete Maßnahmen wirksam umzusetzen.

1 Ziel

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) richtet sich mit einer großen Bandbreite von Veröffentlichungen an IT-Verantwortliche in öffentlicher Verwaltung und Wirtschaft, um sie bei der wirksamen Absicherung ihrer Netze und IT-Systeme zu unterstützen. Mit den hier vorliegenden konkreten und pragmatischen Basismaßnahmen sollen besonders wichtige Einzelthemen in einer übersichtlichen Darstellung zusammengefasst werden, mit denen die kritischsten Handlungsfelder der Cyber-Sicherheit in großen Behörden, Unternehmen und anderen Organisationen charakterisiert werden können. Voraussetzung für die Identifikation dieser Handlungsfelder ist eine möglichst präzise Kenntnis der eigenen Betroffenheit. Hier bietet die separat erhältliche BSI-Empfehlung zur Feststellung der Cyber-Sicherheits-Exposition ein einfach umsetzbares Vorgehen an.

Mit Hilfe der *Cyber-Sicherheits-Exposition* soll das Management unterstützt werden, die reale Betroffenheit herauszuarbeiten, den Schutzbedarf festzustellen und darauf aufbauend das anzustrebende Cyber-Sicherheitsniveau zu definieren. Dabei unterscheidet die *Cyber-Sicherheits-Exposition* zwischen Bedrohungen der Vertraulichkeit, Verfügbarkeit und Integrität und bildet damit die klassischen Schutzziele der Informationssicherheit differenziert ab.

Anhand der Management-Entscheidung ist es dann Aufgabe der Verantwortlichen für IT und IT-Sicherheit (CIO und CISO), Art und Umfang sinnvoller und angemessener Maßnahmen abzuleiten und umzusetzen. Dazu liefern die *Basismaßnahmen der Cyber-Sicherheit* pragmatische Handlungsempfehlungen, deren Beachtung die Grundlagen für robuste Netze und resistente IT-Systeme legt. So werden die Voraussetzungen für eine wirksame Abwehr von Angriffen über das Internet geschaffen.

Mit diesem Vorgehen soll sichergestellt werden, dass angesichts der vielen notwendigen Detailmaßnahmen die wesentlichen Basismaßnahmen der Cyber-Sicherheit stets im Blick behalten werden.

2 Basismaßnahmen zur Cyber-Sicherheit

Die Bestimmung der *Cyber-Sicherheits-Exposition* der zu schützenden Infrastruktur bildet die Voraussetzung für die Planung und Umsetzung angemessener Maßnahmen und ihre anschließende Bewertung auf Notwendigkeit, Angemessenheit und Wirtschaftlichkeit. Mithilfe der im Folgenden dargestellten Basismaßnahmen der Cyber-Sicherheit sollen die Verantwortlichen für IT-Planung und -Betrieb in die Lage versetzt werden, orientiert an der zuvor bestimmten *Cyber-Sicherheits-Exposition* ein angemessenes Cyber-Sicherheits-Niveau zu realisieren.

3 Absicherung von Netzübergängen

Die Absicherung von Netzübergängen ist einer der entscheidenden Faktoren für eine wirksame Abwehr von Angriffen aus dem Internet. Auf Grundlage der Netzstrukturaufnahme müssen Abwehrmaßnahmen für alle Netzübergänge sowie die entsprechenden Prozesse (wie z. B. ein Change Management) geplant und umgesetzt werden.

3.1 Identifikation aller Netzübergänge

Abwehrmaßnahmen in den Netzen bilden bereits ab einer **normalen** *Cyber-Sicherheits-Exposition* einen entscheidenden Faktor zum Schutz vor Angriffen. Wichtig ist dabei die Aufteilung des Netzes in verschiedene Segmente, die sowohl gegeneinander als auch bei der Anbindung an das Internet abgesichert werden müssen.

Dazu sind alle Netzübergänge des Unternehmens oder der Behörde im Rahmen einer *Netzstrukturaufnahme* sowohl im Hinblick auf ihre Anzahl als auch auf die spezifische Art des Übergangs zu identifizieren und zu dokumentieren. Kritisch sind hierbei insbesondere Lösungen, die Schutzmaßnahmen der allgemeinen Netzinfrastruktur umgehen können, etwa:

- individuelle DSL-Zugänge
- UMTS-Datenverbindungen mobiler Geräte
- verschlüsselte Kommunikationswege wie z. B. von IT-Nutzern selbst eingerichtete und genutzte VPN-Verbindungen

Von besonders kritischer Bedeutung sind Zugänge zu Netzen und IT-Systemen für Administratoren, vor allem solche Zugänge, die auch eine Fernwartung/Fernadministration erlauben.

Darüber hinaus sind auch Netzübergänge zwischen verschiedenen Liegenschaften und Anbindungen von Produktivsystemen zu erfassen.

3.2 Segmentierung des Netzes und Minimierung der Übergänge

Voraussetzung für eine in der Praxis umsetzbare und im Betrieb beherrschbare Lösung ist eine am Schutzbedarf unterschiedlicher Bereiche orientierte Netzsegmentierung (z. B. mittels physikalischer Trennung oder VLAN) sowie eine weitgehende Minimierung der externen Netzübergänge. Praxisbeispiele zeigen, dass große Unternehmensnetze mit nur zwei redundanten externen Netzübergängen betrieben werden können.

Eine Umgehung dieser minimierten Zahl an Netzübergängen, z. B. durch parallel betriebene DSL- oder UMTS-Zugänge, muss technisch und organisatorisch unterbunden werden.

3.3 Sicherheitsgateways

Die minimierte Zahl an Netzübergängen muss mit einem geeigneten Sicherheitsgateway abgesichert werden, das mindestens über folgende Eigenschaften verfügt:

- Application Level Gateway bzw. Proxy Firewall
- Intrusion Detection (ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität*)
- Intrusion Prevention (ab einer **sehr hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität*)
- Überprüfung von Datenströmen wie E-Mail, HTTP und FTP auf Schadprogramme
- Möglichkeit für Blacklist- und Whitelist-Lösungen, insbesondere beim Zugriff auf Webseiten

3.4 Schnittstellenkontrolle

Eine Umgehung des Sicherheitsgateways ist durch eine technische Schnittstellenkontrolle auf Client-Systemen, Servern oder weiteren IT-Systemen auszuschließen, um beispielsweise Angriffe über externe Speichermedien (z. B. USB-Speichermedien, Digitalkameras oder MP3-Player) abwehren zu können.

3.5 Absicherung mobiler Zugänge

Mobile IT-Systeme – wie Smartphones oder Laptops – unterliegen einem sehr hohen Verlust- und Diebstahlrisiko. Oftmals kann nicht ausgeschlossen werden, dass mobile IT-Systeme im authentisierten Zustand (d. h. mit angemeldetem Nutzer) abhandenkommen und für Angriffszwecke missbraucht werden.

Daher sind die Berechtigungen, mit denen sich Nutzer über ein mobiles IT-System im Netz bewegen können, auf das unbedingt erforderliche Mindestmaß zu beschränken. Berechtigungen auf Dateiservern und Datenbanken sollten immer nur für die tatsächlich benötigte Zeitspanne und eingeschränkt auf den von außerhalb des Unternehmens oder der Behörde benötigten Bereich gewährt werden.

Verlustfälle mobiler IT-Systeme müssen im Vorfeld eingeplant werden. Reaktive Maßnahmen müssen geübt und im Ernstfall schnell umgesetzt werden, auch außerhalb üblicher Arbeitszeiten. Dazu gehören insbesondere die Löschung des mobilen IT-Systems aus der Ferne, die Sperrung des Zugangs zu den eigenen Netzen für das mobile System und die Einleitung von Lokalisierungsmaßnahmen, um Informationen zum möglichen Verbleib des Geräts erlangen zu können.

4 Abwehr von Schadprogrammen

Die gestaffelte Verteidigung von Angriffen unter dem Einsatz von Schadprogrammen (Viren, Würmer und Trojanische Pferde) muss über eine große Zahl von Systemen verteilt werden. Der eigentliche Client als Arbeitsplatzsystem ist dabei die letzte Verteidigungslinie.

Insbesondere sind Schutzprogramme gegen Schadsoftware auf folgenden Systemen durchgängig einzusetzen:

- Sicherheitsgateway
- E-Mail-Server
- Dateiserver
- mobile und stationäre Arbeitsplatzsysteme

Bei der Auswahl von Schutzprogrammen sollte ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* darauf geachtet werden, dass mehrere Lösungen un-

terschiedlicher Anbieter eingesetzt werden. Verteilt über die verschiedenen Systeme sollten mindestens drei unterschiedliche Lösungen eingesetzt werden. Entscheidend für die Erreichung einer ausreichenden Schutzwirkung ist dabei, dass diese unterschiedlichen Lösungen in der Praxis auf verschiedene Virensignatur-Datenbanken zurückgreifen. Nutzen mehrere Lösungen die gleiche Virensignaturdatenbank, wird keine erhöhte Schutzwirkung durch den Einsatz verschiedener Produkte entfaltet.

Auf dem Sicherheitsgateway sollten ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* verschiedene Lösungen parallel betrieben werden.

Darüber hinaus hat es sich als wertvoll erwiesen, die Installation und ggf. Ausführung von nichtautorisierter Software mit technischen Mitteln zu unterbinden.

Es sollte dauerhaft überprüft werden, ob die eigenen Systeme (z. B. unter Angabe der autonomen Systeme, deren Bestandteil die eigenen IP-Netze sind) in externen Datenbanken (z. B. google.com/webmasters) als gefährlich gekennzeichnet werden. Die Prüfung nach außen angebotener Dienste (insbesondere von Webservern) auf Verteilung von Schadsoftware kann zusätzlich mithilfe eines regelmäßigen Abrufs durch einen automatisierten Crawler und eine anschließende Analyse der heruntergeladenen Inhalte erfolgen.

5 Inventarisierung der IT-Systeme

Zur Planung und anschließenden Umsetzung von Abwehrmaßnahmen auf den eingesetzten IT-Systemen ist zunächst eine vollständige Inventarisierung der eingesetzten IT-Systeme notwendig. Mithilfe dieses Inventarverzeichnisses ist insbesondere zu klären, welche verschiedenen Systemtypen in der Organisation im Einsatz sind.

Leitfragen für die Inventarisierung sind:

- Welche Betriebssysteme und Anwendungen werden auf Servern eingesetzt?
- Welche Betriebssysteme und Anwendungen werden auf stationären und mobilen Clients eingesetzt?
- In welchen Versionen werden die eingesetzten Betriebssysteme und Anwendungen betrieben?
- Welche Patchstände haben die eingesetzten Betriebssysteme und Anwendungen?
- Welche Server werden mit welchem Funktionsumfang, d. h. in welchen Rollen betrieben (Mail-Server, File-Server, Druck-Server, ...)?
- Welche Systeme sind von außerhalb der Organisation über welche Wege erreichbar?

Anhand der Inventarisierung sollte auch die Frage geklärt werden, ob die erhobene Vielfalt an Systemen sicherheitstechnisch und administrativ beherrschbar ist.

6 Vermeidung von offenen Sicherheitslücken

6.1 Patchmanagement

Der überwiegende Teil von Angriffen gegen IT-Systeme erfolgt über Schwachstellen in eingesetzten Softwareprodukten, die in aktuelleren Versionen bereits durch die Hersteller geschlossen wurden. Mit vergleichsweise geringem Aufwand kann daher eine besonders große Schutzwirkung durch ein effizientes Patchmanagement erzielt werden. Aktualisierungen der eingesetzten Software müssen stets kurzfristig installiert werden.

6.2 Stärkere Abwehrmechanismen in aktuellerer Software

Darüber hinaus entwickeln die Hersteller Schutzmaßnahmen in ihren Produkten stetig weiter. Um von erweiterten Schutzmaßnahmen neuerer Produkte zu profitieren, sollte sich die IT-Planung an die (oftmals kurzen) Veröffentlichungszyklen neuer Produktversionen anpassen.

Beispiele für diese notwendige Anpassung sind:

- Die IT-Planung sollte z. B. bei Windows-Betriebssystemen den Veröffentlichungszyklus von Microsoft berücksichtigen und auf die Migration neuer Betriebssystemversionen vorbereitet sein. Gleiches gilt für den Adobe Reader Auch hier sollte immer die neueste Version des Produkts eingesetzt werden, auch dann, wenn Adobe noch ältere Versionen mit Sicherheitsaktualisierungen versorgt.
- Hochkritische Komponenten wie Internet-Browser müssen praktisch permanent auf den neuesten Stand gebracht werden, sodass hier der Ansatz einer „Migrationsplanung" bereits zu kurz greift. Die eigenen Geschäftsabläufe müssen vielmehr stets mit der neuesten Version des eingesetzten Browsers funktionieren, ein Browser sollte dabei mindestens alle sechs Wochen aktualisiert werden. Statt einer Migration auf neue Versionen zu wenigen definierten Zeitpunkten muss in diesem Fall eine laufende Aktualisierung erfolgen.

6.3 Workarounds und Sicherheitsaktualisierungen

Workarounds müssen bei vorhandenen Sicherheitslücken bis zur Verfügbarkeit einer Aktualisierung für ein betroffenes Produkt auf ihre Wirksamkeit in der eigenen Infrastruktur getestet und umgesetzt werden. Bereitgestellte Sicherheitsaktualisierungen müssen anschließend kurzfristig installiert werden. Ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit, Verfügbarkeit* oder *Integrität* ist eine Reaktion auf die Veröffentlichung von Workarounds oder Sicherheitsempfehlungen innerhalb von 72 Stunden unbedingt erforderlich.

7 Sichere Interaktion mit dem Internet

Alle Vorgänge, bei denen Daten und Dienste aus dem Internet abgefragt und verarbeitet werden, sind mit geeigneten Maßnahmen abzusichern. Die jeweilige Stärke der eingesetzten Schutzmechanismen muss dem Schutzbedarf der auf dem jeweiligen IT-System verarbeiteten Daten sowie den einem Angreifer zur Verfügung stehenden möglichen Weiterleitungsmechanismen gerecht werden. Dabei ist insbesondere in Betracht zu ziehen, dass ein zu schützendes System dem Angreifer ggf. nur als Zwischenstation für einen darüber hinaus gehenden Angriff gegen vollkommen andere Ziele im selben Netzsegment dient.

7.1 Sichere Browser

Eine der aus Sicherheitssicht kritischsten Komponenten auf einem IT-System bildet der Internet-Browser. Daher sollte ein besonderes Augenmerk auf dessen Absicherung gelegt werden. Bei Bedarf empfiehlt sich der Einsatz von umgebenden Schutzmechanismen.

In jedem Fall sollte der Browser bereits im Hinblick auf den Speicherschutz seiner eigenen und der von ihm geladenen Komponenten sowie auf die Abschottung besonders gefährdeter Codestellen durch eine Sandbox über starke Sicherheitseigenschaften verfügen.

Ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* sollte der Browser zusätzlich durch eine schützende Umgebung gegen Angriffe aus dem Internet abgeschirmt werden, z. B. durch die Minimierung von Ausführungsrechten oder mithilfe des Einsatzes von Virtualisierungssoftware. Eine Anwendungsvirtualisierung kann nahezu nahtlos in die Betriebssystemumgebung integriert werden.

Für den VS-Bereich zugelassene Lösungen wie die SINA Virtual Workstation bieten sehr starke Absicherungsmechanismen, wenn für die Interaktion mit dem Internet der Browser in eine von den kritischen Daten abgeschottete Sitzung ausgelagert wird. Derartige Lösungen sind ab einer **sehr hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* angeraten.

7.2 Sichere E-Mail-Anwendungen

Im Vergleich zu Browsern können E-Mail-Anwendungen oftmals nicht ähnlich streng von kritischen Daten getrennt werden, da über sie u. a. kritische Daten ausgetauscht werden müssen. Zur Realisierung dieses Austauschs müssen die kritischen Daten aus einer sicheren Dateiablage

in die E-Mail-Anwendung überführt werden, damit sie von dort weiter versandt werden können. Daher muss die E-Mail-Anwendung über einen Zugriff auf solche kritischen Daten verfügen und kann nicht vollständig abgeschottet werden.

Die Abwehr von Angriffen über E-Mails und insbesondere E-Mail-Anhänge erfordert eine zentrale Untersuchung des eingehenden E-Mail-Verkehrs auf Schadprogramme. Hier kann auch auf externe Dienstleister zurückgegriffen werden. Im Falle von Bundesbehörden in den Regierungsnetzen übernimmt das BSI dies als gesetzliche Aufgabe und zentrale Dienstleistung. Bei einer **hohen** oder **sehr hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Verfügbarkeit* von E-Mail ist eine zentrale Filterung von Spam-Nachrichten einzurichten, die sich dynamisch an neue Spam-Wellen anpasst.

Ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* kann neben der Ende-zu-Ende-Verschlüsselung ebenfalls auf externe Dienstleistungen zurückgegriffen werden, die – wie z. B. DE-Mail – Vertraulichkeit und Verbindlichkeit gewährleisten können. Innerhalb eines Unternehmens oder einer Behörde können zentrale Lösungen wie die virtuelle Poststelle eingesetzt werden.

Schließlich kann zur Reduzierung der Angriffsfläche ggf. auch auf eine dedizierte clientseitige E-Mail-Software verzichtet werden und vielmehr eine Webmail-Umgebung im Browser genutzt werden. In solchen Fällen greifen auch für die Darstellung und das Bearbeiten von E-Mails die Schutzmechanismen des Browsers.

7.3 Sichere Darstellung von Dokumenten

So gut wie alle Arbeitsabläufe in Unternehmen und Behörden erfordern eine Darstellung und Bearbeitung von Dokumenten. Für die Darstellung von Dokumenten aus externen Quellen, insbesondere von solchen, die per E-Mail von Personen außerhalb der eigenen Organisation oder als Download aus dem Internet auf dem lokalen System gespeichert worden sind, sollte eine sichere Darstellungsoption verwendet werden. Beispiele sind die „Geschützte Ansicht“ in Microsoft Office 2016 oder der „Geschützte Modus“ ab Adobe Reader X. Darüber hinaus können die Darstellungskomponenten durch Applikationsvirtualisierung noch stärker abgesichert werden.

8 Logdatenerfassung und -auswertung

Oftmals bleiben Sicherheitsvorfälle unerkannt, weil kurzfristig kein sichtbarer oder offensichtlicher Schaden eintritt. Mithilfe eines gut getarnten und hinreichend vorsichtigen Vorgehens ist es Angreifern aber u.U. möglich, über längere Zeiträume die Kontrolle über Zielsysteme zu übernehmen, ohne dass diese Angriffe unmittelbar aufgrund singulärer Ereignisse detektiert werden. Daher ist es notwendig, ebenfalls Verfahren zur Aufdeckung von nicht offensichtlichen Sicherheitsvorfällen und langfristig angelegten Angriffen zu entwickeln.

Eine zentrale Rolle spielt hierbei die regelmäßige Auswertung von Logdaten. Dazu ist bei der IT-Planung ein Konzept zu entwickeln, welche Logdaten auf welchen Systemen erfasst werden müssen, um Angriffe erkennen zu können. Wichtige Quellen für Logdaten sind in jedem Fall das Sicherheitsgateway und die eingesetzten Betriebssysteme.

Insbesondere die auf Intrusion Detection Systemen (IDS) anfallenden Daten sind ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* bei der regelmäßigen Auswertung mit einzubeziehen. Der Einsatz von Lösungen zum Security Information and Event Management (SIEM) ist vorzusehen.

Weitere wichtige Hinweise auf Angriffsversuche liefern Informationen zu anormalen Verhaltensmustern von IT-Systemen, vor allem Daten in Zusammenhang mit Systemabstürzen. Entwickler von Schadsoftware sind in der Regel nicht in der Lage, diese vollkommen zuverlässig

auf allen Zielsystemen zur Ausführung zu bringen. Immer wieder kommt es daher in der Praxis zu Systemabstürzen, deren Logdaten ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* zentral erfasst und auf Hinweise zu Angriffsmustern und Anomalien ausgewertet werden sollten.

9 Sicherstellung eines aktuellen Informationsstands

Die Fähigkeit zur Planung wirksamer Cyber-Sicherheits-Maßnahmen wird im Wesentlichen durch die Qualität und den Umfang des eigenen Informationsstands bestimmt. Daher muss die Versorgung mit aktuellen und fachlich verlässlichen Informationen zur Cyber-Sicherheit sichergestellt werden.

Grundlegend wichtige Informationsquellen sind:

- Warn- und Informationsmeldungen eines etablierten CERT
- Warn- und Informationsmeldungen zu industriellen Steuerungsanlagen (Industrial Control Systems CERT, ICS-CERT)
- Lagebilder von staatlichen Stellen, Herstellern und Sicherheitsdienstleistern
- Warnungen und Sicherheitsempfehlungen von zuständigen Sicherheitsgruppen der jeweiligen Hersteller innerhalb des Unternehmens oder der Behörde eingesetzter Informationstechnik, z. B. des Microsoft Security Response Centers oder des Adobe Product Security and Incident Response Teams

Diese Quellen müssen täglich ausgewertet werden. Kritische Informationen müssen unmittelbar zu Reaktionen führen.

10 Bewältigung von Sicherheitsvorfällen

10.1 Vorbereitung auf Sicherheitsvorfälle

Die Bewältigung von Sicherheitsvorfällen sollte geübt werden, um die Geschäftsabläufe auch unter den erschwerten Bedingungen eines Sicherheitsvorfalls aufrecht erhalten oder zumindest schnell wiederherstellen zu können. Maßnahmen zur Eingrenzung des Schadens müssen bei der IT-Planung konzipiert werden, im Ernstfall schnell umsetzbar sein und eben daher immer wieder geübt werden.

Eine der wichtigsten Maßnahmen dabei ist eine regelmäßige Erstellung von Backups, die im Ernstfall auch tatsächlich wieder zurückgespielt werden können.

10.2 Meldung von Sicherheitsvorfällen

Neben der Bewältigung des eigenen Schadens besteht bei vorsätzlichen Handlungen die Möglichkeit, Strafanzeige zu erstatten, um weitere Vorfälle in anderen Organisationen zu vermeiden und den Polizeibehörden weitergehende Ermittlungen zu ermöglichen.

Darüber hinaus kann sowohl bei vorsätzlichen Handlungen als auch bei gravierenden technischen Problemen (zumindest anonym) eine Meldung an das BSI erfolgen, damit die Informationen zu dem gemeldeten Vorfall in das allgemeine Lagebild einfließen und übergreifende Zusammenhänge erkannt werden können. Nur so kann großflächigen IT-Schadensereignissen koordiniert begegnet werden.

11 Sichere Authentisierung

11.1 Zweifaktor-Authentisierung

Im Rahmen der Authentisierung, für die eine Nutzung eines sicheren Verzeichnisdienstes vorausgesetzt wird, sollte ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit*

oder *Integrität* ein Zweifaktor-Mechanismus verwendet werden. Eine Authentisierung allein mit Nutzername und Passwort ist nicht ausreichend. Schadprogramme wie Trojanische Pferde oder Keylogger greifen unmittelbar die Passwörter ab, sodass auch komplexe Passwörter oder ein häufiger Passwortwechsel keinen hinreichenden Schutz bieten. Wirksam abgewehrt werden solche Angriffe erst mittels eines zweiten, außerhalb des Systems liegenden Faktors wie z. B. eines Hardware-Tokens.

11.2 Trennung von Authentisierungsdaten für verschiedene Aufgaben

Weiterhin sind Bereiche unterschiedlichen Schutzbedarfs zu identifizieren, die in der Folge unterschiedliche Authentisierungen erfordern. Dabei ist besonders auf eine Trennung der Konten von Administratoren und anderen Nutzern zu achten. Unterschiedliche Rollen erfordern verschiedene Authentisierungsdaten. Ergänzend zu der unter *Durchführung nutzerorientierter Maßnahmen* beschriebenen Rollentrennung auch dann, wenn die Rollen von ein und derselben Person wahrgenommen werden. Darüber hinaus dürfen keine gemeinsam genutzten Funktionskonten zur Authentisierung verwendet werden. Die Autorisierung für ein Funktionskonto erfolgt durch die Authentisierung mit einem personenbezogenen Konto.

Die Trennung unterschiedlicher Authentisierungsbereiche ist besonders kritisch in Bezug auf Produktivdatenbanken. Die Authentisierung gegenüber einer Datenbank muss mit der übrigen Authentisierungsstruktur abgestimmt sein. Weder dürfen allgemeine Authentisierungskonzepte durch einen direkten Zugriff auf eine Datenbank umgangen werden können, noch darf die Datenbank selbst ungeschützt bleiben. Native Authentisierungsmechanismen von Datenbanken müssen genutzt werden. Ihre Absicherung darf nicht allein durch die Umgebung erfolgen.

12 Gewährleistung der Verfügbarkeit notwendiger Ressourcen

12.1 Bereitstellung ausreichender eigener Ressourcen

Die wirksame Abwehr von Bedrohungen der Cyber-Sicherheit erfordert die Bereitstellung ausreichender Ressourcen. Diese Aufwände müssen von Unternehmen und Behörden in jeder Phase der IT-Planung und dem anschließenden IT-Betrieb hinreichend berücksichtigt und entsprechende finanzielle und personelle Mittel bereitgestellt werden.

12.2 Einbindung externer Dienstleister

Ein umfassender Schutz ist in der Regel nur durch Einbindung verschiedener externer Dienstleister umsetzbar. Wesentliche Bereiche, in denen auf externen Sachverstand zurückgegriffen werden sollte, sind:

- Durchführung einer herstellerneutralen Cyber-Sicherheitsberatung
- Penetrationstests gegen die eigene IT
- regelmäßige Cyber-Audits
  - Cyber-Quickcheck
  - automatisierte Schwachstellen-Überprüfungen
  - Grundschutz-Audit
- Informationssicherheits-Revisionen
- Analyse und Bewältigung von Sicherheitsvorfällen durch ein externes Computer Emergency Response Team (CERT), sowohl in simulierten Übungsszenarien als auch im Ernstfall
- Durchführung forensischer Maßnahmen

Die Gewichtung und Priorisierung dieser Bereiche sollte auf Grundlage der zuvor bestimmten *Cyber-Sicherheits-Exposition* erfolgen.

Gerade Ressourcen, die erst bei unvorhergesehenen Sicherheitsvorfällen benötigt werden, sollten rechtzeitig eingeplant werden. Bereits lange vor dem tatsächlichen Vorfall muss feststehen, auf welchen externen Dienstleister im Ernstfall verlässlich und kurzfristig zurückgegriffen werden kann.

13 Durchführung nutzerorientierter Maßnahmen

13.1 Sensibilisierung und Schulung

Auch das eigene Personal muss in den Mittelpunkt einer Cyber-Sicherheitsstrategie gerückt werden. Sämtliche technischen Vorkehrungen können durch menschliche Fehler oder bewusste Fehlhandlungen unwirksam werden.

Daher ist das Personal - vom Nutzer der Informationstechnik bis hin zum Administrator, von der Arbeitsebene bis hin zur Leitungsebene, umfassend zu sensibilisieren. Dies gilt auch für die Mitarbeiter von externen Dienstleistern, die in der Organisation eingesetzt werden. Die Sensibilisierung muss sowohl gezielte Schulungen als auch regelmäßige Kurzinformationen zu aktuellen Themen und zur Auffrischungen des notwendigen Wissens während des normalen Arbeitsalltags umfassen. Ein besonderes Augenmerk ist dabei auf Erhalt und Ausbau der Kompetenz von Administratoren zu legen.

13.2 Rollentrennung

Die Personalplanung muss zudem in Bezug auf die eingesetzte IT folgende Aspekte umfassen:

- Definition der technischen und organisatorischen Rollen
- Klärung von Verantwortlichkeiten eines jeden Einzelnen
- Festlegung von Zuständigkeiten (auch unter Einbeziehung externer Dienstleister)

Diese Planung soll eine klare Trennung von Rollen vorsehen. Eine Konzentration vieler oder aller Zuständigkeiten in einer Rolle sollte immer vermieden werden.

14 Sichere Nutzung Sozialer Netze

Neben den IT-Systemen, die unter der direkten Kontrolle des Unternehmens bzw. der Behörde stehen, gewinnen externe Dienste wie Soziale Netze eine zunehmende Bedeutung für bestimmte Geschäftsabläufe, insbesondere im Bereich des Marketings oder der Öffentlichkeitsarbeit.

Der sichere und damit auch seriöse Auftritt einer Organisation sowie die (beruflichen) Profile der Beschäftigten in Sozialen Netzen wie Facebook, Google+ und Xing ist daher in die IT-Planung einzubeziehen. Die Sensibilisierung von Mitarbeitern muss insbesondere das Verhalten in Sozialen Netzen in Form verbindlicher Vorgaben (Social Media Guidelines) und durch Aufklärungsmaßnahmen umfassen.

Sicherheitsmaßnahmen, die von den Betreibern der Sozialen Netze angeboten werden, müssen bekannt sein und so wirksam wie möglich genutzt werden. Dabei müssen gerade auch die Grenzen der IT-Sicherheit, die in Sozialen Netzen umsetzbar ist, stets allen Nutzern innerhalb der Organisation verdeutlicht werden. Existieren direkte Schnittstellen zwischen Sozialen Netzen und der organisationseigenen Infrastruktur, so sind diese Übergänge besonders abzusichern. Falls dies nicht möglich ist, sind diese Übergänge im Zweifel zu trennen.

15 Zusatzmaßnahmen bei höherer Cyber-Sicherheits-Exposition

Die Verfügbarkeit, Vertraulichkeit und Integrität von Informationstechnik bilden die klassischen Grundwerte für einen sicheren Betrieb. In Abhängigkeit des individuellen Schutzbedarfs eines Systems, Netzsegments oder der gesamten Organisation sind zur Gewährleistung dieser Grundwerte zusätzliche Maßnahmen erforderlich. Die Notwendigkeit folgt insbesondere aus der oben beschriebenen Feststellung der *Cyber-Sicherheits-Exposition*, sobald **hohe** oder **sehr hohe** Werte in Bezug auf *Vertraulichkeit, Verfügbarkeit* oder *Integrität* festgestellt werden.

15.1 Verfügbarkeit

Falls für die *Cyber-Sicherheits-Exposition* (*Verfügbarkeit)* ein Wert von **hoch** oder **sehr hoch** bestimmt wurde, muss die notwendige Verfügbarkeit von Informationstechnik primär durch Schaffung von Redundanzen erzielt werden. Dazu sind auf allen Ebenen Komponenten zu identifizieren, die für eine Aufrechterhaltung des Geschäftsbetriebs erforderlich sind. Diese Komponenten müssen orientiert an den jeweiligen Verfügbarkeitsanforderungen individuell hinreichend redundant ausgelegt werden. Konkret sind z. B. geschäftskritische Systeme mehrfach vorzuhalten, die Netzanbindung an das Internet muss über voneinander unabhängige Übergangsstellen erfolgen, zwischen denen nahtlos gewechselt werden kann. Ebenso muss es möglich sein, bei Ausfall des Providers den Internetzugang kurzfristig über einen alternativen Provider zu realisieren. Entsprechende Dienstleistungen müssen präventiv gebucht und deren Verfügbarkeit regelmäßig getestet werden.

Diese Redundanzanforderungen beinhalten auch die ständige Verfügbarkeit eines zweiten Internet Browsers, falls der üblicherweise genutzte Browser aufgrund von kritischen Sicherheitslücken zeitweise nicht genutzt werden kann. In solchen Fällen muss schnell auf ein alternatives Produkt gewechselt werden können, da die Nutzung eines Browsers, der über bekannte Sicherheitslücken über das Internet erfolgreich angegriffen werden kann, ausschließbar sein muss.

Zur Gewährleistung der Verfügbarkeit von nach außen angebotenen Diensten, insbesondere der Verfügbarkeit von Internetangeboten und E-Mail, sind Maßnahmen gegen Distributed-Denial-of-Service-Angriffe (DDoS) zu implementieren. Zur Abwehr solcher Angriffe kann auch auf externe Dienstleister zurückgegriffen werden. Im Rahmen der Prävention sind diese externen Dienstleistungen vorab einzukaufen. Sowohl interne als auch externe Maßnahmen sind regelmäßig zu üben.

15.2 Vertraulichkeit

Einer *Cyber-Sicherheits-Exposition (Vertraulichkeit)* mit einem Wert von **hoch** oder **sehr hoch** wird vor allem durch Einsatz kryptographischer Verfahren begegnet. Dies gilt sowohl für die Verschlüsslung von E-Mails und Dokumenten als auch für die Absicherung von Festplatten – vor allem in mobilen IT-Systemen. Hierfür sind Festplatten vollständig mit wirksamen kryptographischen Mitteln zu verschlüsseln.

15.3 Integrität

Neben den Primärzielen des Angreifers, die vor allem die Verfügbarkeit und Vertraulichkeit gefährden, kann es bei mehrstufigen und langfristig durchgeführten Angriffen auch um die Manipulation von Datenbeständen gehen, sodass die *Cyber-Sicherheits-Exposition* in Bezug auf die *Integrität* mit **hoch** oder **sehr hoch** zu bewerten ist. Dieser Bedrohung der Integrität ist frühzeitig durch integritätssichernde Maßnahmen, wie der kryptographischen Signatur zu begegnen.

Neben der Kommunikation ist jedoch auch die Integrität der IT-Systeme selbst eines der wichtigen Schutzziele. Dazu müssen sowohl während der Beschaffung als auch im Betrieb verschiedene technische und organisatorische Maßnahmen umgesetzt werden, z. B.

- der Einsatz von Trusted Boot oder Secure Boot
- IT-Revisionen
- bereits im Vorfeld des Betriebs ein auf Sicherheit ausgerichtetes Supply-Chain-Management

15.4 Durchführung von Penetrationstests

Ab der *Cyber-Sicherheits-Exposition* **hoch** ist die Durchführung regelmäßiger Penetrationstests angebracht. Diese sollten von Experten, die nicht an der Planung der IT beteiligt waren, durchgeführt werden. Aufwand und Intensität des Penetrationstests sind der Exposition anzupassen.

15.5 Unterstützende Maßnahmen zur Abwehr gezielter Angriffe

Die *Cyber-Sicherheits-Exposition* eines Unternehmens oder einer Behörde bildet ein gutes Maß für die Wahrscheinlichkeit, in das Zielspektrum von Angeifern zu geraten. Dabei sind solche Täterkreise von besonderer Relevanz, denen es nicht um ungerichtete Breitenangriffe gegen mehr oder minder wahllose Ziele geht, sondern die es vielmehr gezielt auf eine bewusst ausgewählte Organisation abgesehen haben. Die Abwehr solcher gezielter Angriffe gegen die Vertraulichkeit oder die Verfügbarkeit, deren Techniken von Angreifern auf die spezielle Situation der angegriffenen Organisation angepasst werden können, stellt eine der größten Herausforderungen der Cyber-Sicherheit dar.

Eine gestaffelte Verteidigung im koordinierten Zusammenspiel der hier aufgezeigten Maßnahmen ist in der Lage, auch gezielte Angriffe massiv zu erschweren.

Bei höherem Schutzbedarf, d. h. einer *Cyber-Sicherheits-Exposition (Vertraulichkeit* und/oder *Verfügbarkeit)* mit Werten von **hoch** oder **sehr hoch***,* sollte darüber hinaus auch der Einsatz speziell gehärteter (auch alternativer) Betriebssysteme und Anwendungen in Betracht gezogen werden. Die Verwendung von Standardkonfigurationen im Bereich der Betriebssysteme und Anwendungen erleichtern gezielte Angriffe deutlich. Ziel muss es daher sein, die Vorhersagbarkeit von Plattformeigenschaften weitestgehend auszuschließen.

Wenn in der Risikoabschätzung deutlich wird, dass Schutzmechanismen an Netzübergängen nicht in der Lage sind, erwartete gezielte Angriffe abzuwehren, sind zudem Netze, in denen die zu schützenden Daten verarbeitet werden, vollständig von der Umgebung zu trennen.

16 Checkliste zu den Basismaßnahmen der Cyber-Sicherheit

Folgende Checkliste fasst die Umsetzung der Basismaßnahmen der Cyber-Sicherheit zusammen:

- ☐ Der Bedrohungsgrad der eigenen Infrastruktur sowie die Transparenz der Institution gegenüber Angreifern wurde bestimmt. Daraus wurde die *Cyber-Sicherheits-Exposition* abgeleitet.
- ☐ Sämtliche Netzübergänge sind identifiziert und hinreichend abgesichert.
- ☐ Die Infektion mit Schadprogrammen wird mit wirksamen Maßnahmen unterbunden.
- ☐ Die IT-Systeme wurden inventarisiert und auf ihre sicherheitstechnische Beherrschbarkeit hin geprüft.
- ☐ Offene Sicherheitslücken auf IT-Systeme werden vermieden.
- ☐ Eine Interaktion mit dem Internet findet nur über abgesicherte Komponenten statt.
- ☐ Logdaten werden zentral erfasst und ausgewertet.
- ☐ Die eigene Organisation wird mit allen notwendigen Informationen versorgt.
- ☐ Die Organisation ist auf die Bewältigung von Sicherheitsvorfällen vorbereitet.
- ☐ Die eingesetzten Mechanismen zur Authentisierung verhindern eine missbräuchliche Nutzung durch Dritte.
- ☐ Es stehen ausreichende interne Ressourcen zur Verfügung, externe Dienstleister werden eingebunden.
- ☐ Das eigene Personal wird in Fragen der Cyber-Sicherheit qualifiziert und sensibilisiert.
- ☐ Es werden nutzerorientierte Maßnahmen zur Rollentrennung durchgesetzt.
- ☐ Die Organisation und ihre Mitglieder bewegen sich sicher in Sozialen Netzen.
- ☐ Bei höherem Schutzbedarf werden Vertraulichkeit, Verfügbarkeit und Integrität durch wirksame Maßnahmen gewährleistet und Penetrationstests durchgeführt.
- ☐ Zur Abwehr gezielter Angriffe werden unterstützende Schutzmaßnahmen ergriffen.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.