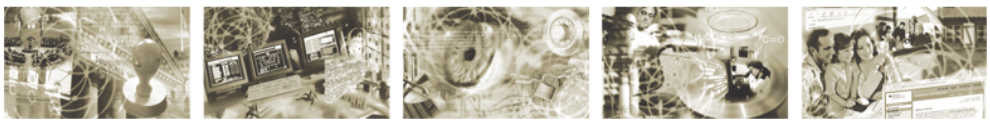
Bundesamt
für Sicherheit in der
Informationstechnik



Eckpunktepapier

Mindestanforderungen zur Informationssicherheit bei eCommerce-Anbietern

Version 1.2

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

0 Einleitung

0.1 Motivation

Die weltweite Nutzung des Internets hat das tägliche Leben einschneidend verändert. Zunehmend nutzen Bürger das Internet für die private Lebensgestaltung, die täglichen Einkäufe und Dienstleistungen. Die massiv steigenden Umsätze im eCommerce verdeutlichen diesen Trend.

Mit der Nutzung des Internets als Kommunikationsmedium für Einkäufe und damit verbundene Zahlungsvorgänge werden bei eCommerce-Anbietern in großem Umfang personenbeziehbare Daten übertragen und verarbeitet. Diese Daten besitzen einen hohen Bedarf an Vertraulichkeit:

- sie beinhalten Namen, Rechnungs- und E-Mail-Adressen,
- sie spiegeln das Kaufverhalten, die Interessen und Neigungen der Kunden wider,
- sie ermöglichen die Authentisierung der Kunden und damit den persönlichen Zugang zu den eCommerce-Angeboten
- sie dienen der Abwicklung des Zahlungsverkehrs.

Dem gegenüber muss berücksichtigt werden, dass die stark steigende Cyber-Kriminalität gerade an diesen Daten aufgrund des hohen Missbrauchspotenzials großes Interesse hat. Angreifer nutzen solche Daten, um finanzielle Vorteile zu erlangen, SPAM zu verteilen oder mit Social Engineering vorbereitete gezielte Attacken zu verursachen. Daher kommt dem eCommerce-Anbieter, der diese Daten erhebt, verarbeitet und speichert, eine hohe Verantwortung zu, den ausreichenden Schutz dieser Daten zu gewährleisten.

Dabei muss bedacht werden, dass die Aufwände für die notwendige Informationssicherheit mit dem Umfang der gespeicherten Daten und der Kundenzahl skaliert, denn je mehr aus Cyber-Kriminellen-Sicht lohnende Daten vorhanden sind, desto interessanter und lukrativer ist das Angriffsziel. Daher müssen insbesondere eCommerce-Anbieter mit Hunderttausenden oder Millionen von Kundendatensätzen ein umfassendes und ausgereiftes Informationssicherheits-managementsystem mit adäquaten Sicherheitsmaßnahmen implementieren und aufrechterhalten.

0.2 Zielsetzung

Verschiedene erfolgreiche Cyber-Angriffe zeigen, dass Cyber-Kriminelle mit raffinierten technischen Methoden Fehler und Schwachstellen in angegriffenen Zielsystemen suchen und ausnutzen. Die technische Komplexität der Zielsysteme, die Vielfalt der eingesetzten Produkte und die Schnelllebigkeit der Dienste erschweren jedoch die Verteidigung gegen diese Angriffe. Dem

Angreifer genügt es, lediglich eine einzige ausnutzbare Schwachstelle zu finden. Im Umkehrschluss müssen alle IT-Systeme im eCommerce vollständig gesichert und überwacht werden, um eine möglichst geringe Angriffsfläche zu bieten.

Dabei muss beachtet werden, dass nicht nur die unmittelbar für die Abwicklung des eCommerce sichtbaren IT-Systeme Ziel der Angriffe sein können. Sämtliche nachgelagerten IT-Systeme des eCommerce-Anbieters, die funktional Zugriff auf die Daten und Prozesse nehmen können (z. B. Systeme zur Administration, Pre- und Postprocessing, Marketing, Logistik, Zahlungsverkehr etc.) können für Angriffe missbraucht werden.

Informationssicherheit in solch komplexen IT-Systemen zu gewährleisten, ist eine große Herausforderung. Das BSI hat daher basierend auf dem Stand der Technik Mindestanforderungen zur Informationssicherheit von eCommerce-Systemen zur Orientierung erstellt. Sie richten sich insbesondere an Anbieter, die einen großen Kundenstamm haben und damit im Fokus von Cyber-Kriminellen sind. Das vorliegende Eckpunktepapier kann von eCommerce-Anbieter als Richtschnur für die Umsetzung von Sicherheitsmaßnahmen für unter eigener Regie als auch für durch Dritte im Auftrag betriebene IT-Systeme genutzt werden.

Das Eckpunktepapier stellt einen Überblick über die wesentlichen Faktoren für eine angemessene Informationssicherheit im eCommerce dar. Dazu gehören:

- Informationssicherheitsmanagement,
- Konzeption der Sicherheitsarchitektur,
- Umsetzung der Informationssicherheitsmaßnahmen und
- die Aufrechterhaltung des sicheren Betriebs.

Das vorliegende Dokument betrachtet nicht nur eCommerce-spezifische Aspekte, sondern richtet den Blick auch auf grundlegende Anforderungen der Informationssicherheit, auf die alle eCommerce-Dienste aufsetzen sollten. Die Empfehlungen wurden weitgehend abstrakt gehalten, ohne detaillierte Anweisungen für deren Umsetzung zu geben. Dies würde zum einen den Umfang des Dokuments sprengen und zum anderen lässt dies die Vielfältigkeit der eCommerce-Angebote nicht zu. Die Umsetzung der Sicherheit eines bestimmten Angebots muss daher immer individuell erfolgen. Für die Umsetzung der Mindestanforderungen hilfreiche weiterführende konkretisierende Empfehlungen und Standards werden am Ende des Dokuments aufgeführt.

1 Informationssicherheitsmanagement beim Anbieter

Für ein zuverlässiges und sicheres eCommerce-Angebot ist als Grundlage ein effizientes Management der Informationssicherheit (Information Security Management System, ISMS) auf Seiten des eCommerce-Anbieters unerlässlich. Das BSI empfiehlt, sich für Aufbau und Betrieb eines ISMS an ISO 27001/2 oder bevorzugt am BSI-Standard 100-2 zur IT-Grundschutz-Vorgehensweise (der ISO 27001/2 abdeckt) zu orientieren.

Wesentliche Bestandteile eines ISMS sind eine funktionierende Sicherheitsorganisation und ein Informationssicherheitskonzept als Werkzeuge des Managements zur Umsetzung der Sicherheitsstrategie. Informationssicherheit ist ein Prozess und sollte daher im Sinne eines PDCA-Zyklus (Plan-Do-Check-Act) fortlaufend weiterentwickelt werden.

Damit eCommerce-Anbieter nachweisen können, dass sie auch bei hohem Schutzbedarf bezüglich Vertraulichkeit und Verfügbarkeit ausreichend Sicherheit gewährleisten, ist eine Zertifizierung des Informationssicherheitsmanagements sinnvoll. Vorzugsweise sollte dies nach ISO 27001 auf Basis von IT-Grundschutz, ISO 27001 oder einem anderen etablierten Standard erfolgen.

2 Sicherheitsarchitektur

Soll eine eCommerce-Plattform wirksam abgesichert werden, müssen alle Aspekte betrachtet werden, die die Vertraulichkeit, Integrität und Verfügbarkeit der dort gespeicherten Informationen gefährden können. Neben einem gut strukturierten Vorgehensmodell für alle IT-Prozesse ist insbesondere der Aufbau einer Sicherheitsarchitektur zum Schutz der Daten, Anwendungen, IT-Systeme und Netze von Bedeutung.

2.1 Physische Sicherheit

Rechenzentren sind die technische Basis von eCommerce-Systems. Insofern ist es wichtig, dass jeder eCommerce-Anbieter die Sicherheit seiner Anlagen nach dem aktuellen Stand der Technik gewährleistet. Dazu zählt eine wirksame Zutrittskontrolle zu allen Räumlichkeiten, in denen sich Geräte oder Daten befinden, die für das eCommerce-Angebot genutzt werden (z. B. permanente Überwachung der Zugänge, etwa durch Videoüberwachungssysteme, Bewegungssensoren, Alarmsysteme und geschultes Sicherheitspersonal).

Im Eigeninteresse ist eine ausreichende Verfügbarkeit zu gewährleisten. Daher sollten Versorgungskomponenten, die für den Betrieb unverzichtbar sind, redundant ausgelegt sein, so zum Beispiel die Stromversorgung, Klimatisierung und Internet-Anbindung. Auch zeitgemäße Vorkehrungen für den Brandschutz müssen umgesetzt sein und regelmäßig getestet werden. Ein Rechenzentrum sollte insgesamt einen Sicherheitsbereich bilden, der sowohl ausreichend vor Elementarschäden, z. B. durch Gewitter oder Hochwasser, als auch vor unbefugtem Eindringen schützt.

2.2 Sicherheit von IT-Systemen

IT-Systeme (Server, Clients, Netzkomponenten) sollten mit einer sicheren Grundkonfiguration betrieben werden, um diese gegen Angriffe über das Netz und gegen unautorisierte lokale Zugriffe abzusichern. Hierzu sollten die vom Hersteller gesetzten Standardeinstellungen zum Beispiel für Benutzerkonten (Standard-Passwörter, Namen von administrativen Benutzern etc.) geändert und nicht benötigte Benutzerkonten gelöscht bzw. deaktiviert werden. Des Weiteren sollte die Nutzung mobiler Datenträger über externe Schnittstellen mittels geeigneter Mechanismen kontrolliert und das Booten über externe Datenträger unterbunden werden.

Weiterhin sollten Applikationen und Netzdienste, die zum Betrieb des IT-Systems nicht erforderlich sind, ebenfalls deaktiviert oder deinstalliert werden. Auf allen stationären und mobilen Clients und allen durch Schadsoftware potenziell betroffenen Servern sollte Software zur Erkennung von Schadprogrammen genutzt werden, die regelmäßig aktualisiert und durch den Einsatz eines

lokalen Paketfilters wie zum Beispiel Personal Firewalls ergänzt wird.

Auf IT-Systemen, die besonders schützenswerte Daten verarbeiten, sollte darüber hinaus ein Verfahren zum Integritätsschutz eingesetzt werden, um eine Kompromittierung des Systems zeitnah erkennen zu können.

Sicherheitsrelevante Ereignisse müssen revisionssicher protokolliert und regelmäßig ausgewertet werden (siehe hierzu auch Kapitel 4 „Monitoring und Security Incident Management“). Sicherheitsrelevante Patches und Updates für Betriebssysteme und Applikationen müssen über ein kontrolliertes Patch- und Änderungsmanagement unverzüglich eingespielt werden (siehe hierzu auch Kapitel 2.6 „Patch- und Änderungsmanagement“).

Ist es für den Betrieb einer eCommerce-Plattform notwendig, dass auf der Seite des Kunden bestimmte Sicherheitsmaßnahmen umgesetzt werden müssen, so muss der Kunde darüber ausführlich informiert werden.

2.3 Netzsicherheit

2.3.1 Netzkonzeption

Grundlage eines sicheren eCommerce-Angebots ist eine sichere Netzkonzeption. Sichergestellt sein muss, dass sämtliche IT-Komponenten des eCommerce-Angebots nicht unmittelbar mit dem Internet verbunden sind, sondern durch Sicherheitsgateways geschützt sind.

In der Regel handelt es sich bei eCommerce-Angeboten um komplexe, webbasierte IT-Infrastrukturen, die aus Webserver, Webanwendungsserver sowie Datenbanken und ggf. weiteren Hintergrundsystemen bestehen. Der Zugriff über das Internet erfolgt auf den Webserver. Um nutzerspezifische Inhalte generieren zu können, kommuniziert der Webserver (WWW) mit dem Webanwendungsserver (WWW AS) und liefert dessen Ergebnisse aus. Dazu benötigt der Webanwendungsserver Zugriff auf die in den Hintergrundsystemen hinterlegten Daten oder generiert dort neue Datensätze.

Um derartige komplexe IT-Infrastrukturen abzusichern, ist eine Separierung der verschiedenen Bereiche (Webserver, Webanwendungsserver und Hintergrundsysteme) in unterschiedliche Schutzzonen, wie beispielhaft in Abbildung 1 dargestellt, empfehlenswert. Die Trennung erfolgt hier durch Sicherheitsgateways, im einfachsten Fall mittels Paketfilter (PF). Eine solche Infrastruktur ermöglicht bei entsprechender Konfiguration (nur benötigte Kommunikationsbeziehungen freigeschaltet), dass aus dem Internet nur auf den Webserver zugegriffen werden kann, nicht aber auf die datenverarbeitenden Systeme. Auch sollten die datenverarbeitenden Systeme selbst nicht mit dem Internet kommunizieren dürfen

(ausgenommen sind ggf. Systeme zum Versand von E-Mails).

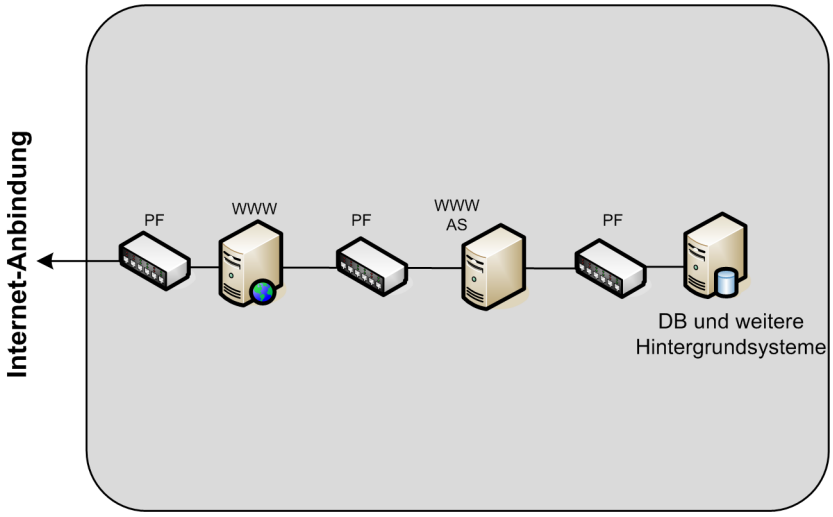


Abbildung 1: Beispiel für den Aufbau einer sicheren eCommerce-Netzinfrastruktur

2.3.2 Netzabsicherung

Um Angriffe auf Kundendaten zu verhindern, sollte jeder Anbieter wirksame Sicherheitsmaßnahmen zur Abwehr netzbasierter Angriffe umsetzen. Zusätzlich zu gängigen IT-Sicherheitsmaßnahmen wie Schutz vor Schadprogrammen, Spam-Schutz, Sicherheitsgateways, IDS/IPS-Systemen, sollte insbesondere auch darauf geachtet werden, dass jegliche Kommunikation zwischen eCommerce-Angebot und Kunden, für Fernadministration und mobiles Arbeiten sowie zwischen den Standorten des Anbieters verschlüsselt ist. Sind zudem weitere externe Dienstleister eingebunden, dann ist die Kommunikation mit ihnen ebenfalls zu verschlüsseln.

Aufgrund der Konzentration der Ressourcen in zentralisierten Rechenzentren ist ein besonders für eCommerce-Angebote gefährlicher Angriff die Ausführung von Distributed Denial of Service-Angriffen (DDoS-Angriffen). Mittlerweile erreichen DDoS-Angriffe (wie beispielsweise die DNS Amplification/Reflection Attack) enorme Bitraten (über 100 Gbps). Ein Standard-Backbone ist für eine weit geringere Datenrate ausgelegt. Folglich können viele eCommerce-Anbieter DDoS-Angriffe mit hohen Datenraten kaum abwehren. Vor diesem Hintergrund sollte jeder Anbieter im Eigeninteresse über geeignete Maßnahmen zur Abwehr von DDoS (DDoS-Mitigation) entscheiden. Aufgrund der Tatsache, dass viele Anbieter DDoS-Angriffe mit hohen Datenraten selbst kaum abwehren können, bietet es sich an, solche Mitigation-Dienste über größere Internet Service Provider (ISPs) einzukaufen und deren Nutzung in Verträgen zu regeln.

2.3.3 IT-System-Management

Das Management der zum eCommerce-Angebot gehörenden IT-Systeme sollte über ein getrenntes Out-of-Band-Management-Netz erfolgen. Eine verschlüsselte Übertragung von Management-Protokollen, die bei In-Band-Management aus Sicherheitsgründen unverzichtbar ist, bereitet häufig Probleme beim Passieren von Sicherheitsgateways. Durch die Trennung von Nutz- und Steuerkanälen kann das Eindringen, Abhören und Stören der IT-Systeme und Kommunikationsverbindungen deutlich erschwert werden. Auch im Falle einer Störung bietet das getrennte Management bessere Möglichkeiten zur Beseitigung.

2.3.4. Mobiler Zugriff

Für Fernadministration der eCommerce-Infrastruktur ist sicherzustellen, dass diese Zugriffe über ein dediziertes „Out-of-Band“ Management-Netz erfolgen (siehe hierzu auch Kapitel 2.3.3 „IT-System-Management“), welches durch eine geeignete Segmentierung vollständig von anderen Teilen des Netzes getrennt ist. Mittels Access Control Lists (ACLs) sollte der Zugriff auf das Management-Interface der IT-Systeme nur einer dedizierten Management-Station möglich sein und alle nicht benötigten Dienste auf den Management-Interfaces deaktiviert werden. Zur Fernadministration sollten ausschließlich sichere Protokolle verwendet werden, die über eine angemessene Verschlüsselung verfügen (z.B. SSH, IPSec).

Wenn Mitarbeiter auf die eCommerce-Systeme und -Datenbestände mittels mobiler Geräte zugreifen soll, ist eine starke Authentisierung gegenüber dem mobilen Gerät und dem Unternehmensnetz zu gewährleisten und die Kommunikation zu verschlüsseln.

Die für den mobilen Zugriff genutzten mobilen Endgeräte (Laptop, Smartphone etc.) sollten ebenfalls den in Kapitel 2.2 „Sichere IT-Systeme“ genannten Anforderungen an eine sichere Grundkonfiguration entsprechen und darüber hinaus über eine Verschlüsselung der lokalen Datenspeicher verfügen.

2.4 Anwendungssicherheit

2.4.1 Datensparsamkeit

Um Cyber-Kriminellen eine möglichst geringe Angriffsfläche zu bieten, ist in der Konzeption und Realisierung von eCommerce-Angeboten von Beginn an die Maxime der Datensparsamkeit zu beachten. Generell sollten nur solche Daten erhoben, verarbeitet und gespeichert werden, die für die Abwicklung des eCommerce notwendig sind. Altdatenbestände, für die keine Speicherungsnotwendigkeiten mehr bestehen, sind sicher zu löschen.

2.4.2 Sichere Software-Entwicklung

Bei der Software-Entwicklung für eCommerce-Anwendungen muss Sicherheit als fester Bestandteil des Software Development Life Cycle Prozess (SDLC-Prozess) etabliert werden. Sicherheitsaspekte müssen in allen Phasen des Software-Entwicklungsprozesses berücksichtigt werden und es dürfen nur Programme bzw. Module zum Einsatz kommen, die ordnungsgemäß getestet und auch seitens der Sicherheitsverantwortlichen freigegeben wurden.

Da eCommerce-Anwendungen in der Regel auf Web-Technologien aufsetzen, kommt der Sicherheit der Anwendungen gegen Angriffe auf Applikationsebene eine große Bedeutung zu. Daher sollte sichergestellt werden, dass bei der Entwicklung die Prinzipien der Web Application Security eingehalten werden. Dazu gehört beispielsweise die Einhaltung des Minimalprinzips. Benutzereingaben sind stets als potenziell gefährlich einzustufen und müssen daher Server-seitig gefiltert werden, um Cross-site scripting (XSS), SQL-Injection, Cross-site request forgery, etc. zu verhindern.

Zur Überprüfung der Software können neben Code Reviews zusätzlich auch automatische Review-Tools eingesetzt sowie Vulnerability Tests durchgeführt werden.

2.4.3 Sichere Datenspeicherung

Der Lebenszyklus von Daten umfasst ihre Erzeugung, die Datenspeicherung, die Datennutzung und -weitergabe und das Löschen der Daten. Alle diese Phasen im Daten-Lebenszyklus sollte jeder eCommerce-Anbieter mit entsprechenden Sicherheitsmechanismen unterstützen.

Zur Vermeidung von Datenverlusten sollte jeder eCommerce-Anbieter regelmäßige Datensicherungen basierend auf einem unternehmensweiten Datensicherungskonzept durchführen und die Datenträger in einer sicheren Umgebung aufbewahren.

Jeder eCommerce-Anbieter muss eine effektive Vorgehensweise zum sicheren Transport, Löschen bzw. Vernichten von Daten und Datenträgern haben.

2.5 Verschlüsselung und Schlüsselmanagement

Im Bereich eCommerce ist die Verschlüsselung personenbeziehbarer Daten ein zentrales Sicherheitselement:

- Sämtliche personenbeziehbaren Daten und Daten zur Abwicklung des Zahlungsverkehrs sind während der Übertragung über unsichere Kommunikationswege, insbesondere im Internet, hinreichend sicher zu verschlüsseln. Dies kann mittels geeigneterer TLS/SSL- oder IPSEC-Implementierungen erreicht werden. Die eCommerce-Server sollten mit verifizierbaren Zertifikaten ausgestattet sein.

- Kundendaten mit einem besonders hohen Missbrauchspotenzial (Kennungen, Passwörter, Informationen zur Abwicklung des Zahlungsverkehrs, etc.) sind verschlüsselt zu speichern.

Um schutzbedürftige Informationen sicher speichern, verarbeiten und transportieren zu können, sollten geeignete kryptographische Verfahren und Produkte eingesetzt werden. Es müssen in jeder Lebenszyklus-Phase eines kryptographischen Schlüssels geeignete Sicherheitsmaßnahmen umgesetzt werden, damit Schlüssel vertraulich, integer und authentisch erzeugt, gespeichert, ausgetauscht, genutzt und vernichtet werden. Da beim Einsatz kryptographischer Verfahren sehr viele komplexe Einflussfaktoren zu betrachten sind, sollte hierfür ein unternehmensweites Kryptokonzept mit Schlüsselmanagement erstellt werden.

2.6 Patch- und Änderungsmanagement

Unverzichtbar ist ein gut eingespieltes und effektives Patch- und Änderungsmanagement für alle IT-Systeme, damit Störungen im Betrieb vermieden sowie Sicherheitslücken minimiert bzw. unverzüglich beseitigt werden können. Zur Qualitätssicherung und um Fehler zu erkennen beziehungsweise zukünftigen Fehlern vorbeugen zu können, sollte grundsätzlich jeder Patch und jede Änderung, bevor sie aufgespielt werden, ausreichend getestet und ihre Wirksamkeit bewertet werden. Die Installation von Software sowie Konfiguration außerhalb des Änderungsmanagements muss unterbunden werden. Das Sicherheitsmanagement muss in geeigneter Weise in das Patch- und Änderungsmanagement einbezogen werden.

3 Identitäts- und Berechtigungsmanagement

Das Identitäts- und Berechtigungsmanagement ist ein wichtiger Bestandteil der Zugriffskontrolle. Ein eCommerce-Anbieter muss dieses mit geeigneten organisatorischen, personellen und technischen Maßnahmen absichern. Dies gilt sowohl für die Kunden des eCommerce-Anbieters wie auch in besonderem Maß für dessen Mitarbeiter.

Die eCommerce-Anwendung wird von vielen Kunden in Anspruch genommen. Aufgabe des Identitäts- und Berechtigungsmanagements ist es, dafür zu sorgen, dass nur befugte Personen die zur Verfügung gestellten Funktionen nutzen können. Hier ist, je nach Art der Anwendung, ein sicherer Zugriff auf die eCommerce-Anwendung durch den Anbieter zur gewährleisten. Zur Authentisierung ist mindestens ein erzwungen sicheres Passwort (Komplexität, Länge) zu verwenden, es kann aber auch eine Zwei-Faktor-Authentisierung sein, wie es zum Beispiel beim Online-Banking üblich ist.

Für die Mitarbeiter des eCommerce-Anbieters sollten angemessen hohe Sicherheitsstandards für die Authentisierung gelten. Insbesondere für Administratoren und andere „extremely privileged users“ ist anzustreben, dass sie nur nach einer Zwei-Faktor-Authentisierung Zugriff auf die Systeme des Anbieters erhalten. Hier bieten sich z. B. Hardware-basierte Authentisierung mit Chipkarten oder USB-Sticks oder Einmal-Passwörter, die auch von Hardwaregeräten generiert werden können, an. Und schließlich sollten besonders kritische Administrationstätigkeiten nur im Vier-Augen-Prinzip durchführbar sein.

Das Rechtemanagement muss auf einem Rollenkonzept basieren, das gewährleistet, dass jede Rolle nur die Daten (auch Metadaten) sehen darf, die zur Erfüllung der Aufgabe notwendig sind. Die eingerichteten Rollen, die Zugehörigkeit der Mitarbeiter zu diesen Rollen und die mit der Rolle verbundenen Rechte sollten regelmäßig überprüft werden. Generell sollte das „least privilege“-Model genutzt werden, sodass die Mitarbeiter und privilegierten Nutzer nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgaben benötigen. Dies gilt in besonderem Maß für den Zugriff auf die Kunden-Daten.

4 Monitoring und Security Incident Management

Die Beurteilung der operationellen Sicherheit einer eCommerce-Plattform setzt ein umfassendes Monitoring voraus. Um die Informationssicherheit im laufenden Betrieb aufrecht zu erhalten, ist es notwendig, die Behandlung von Angriffen bzw. Sicherheitsvorfällen im Vorfeld zu konzipieren und einzuüben. Abhängig von den Sicherheitsanforderungen sollte geprüft werden, ob der eCommerce-Dienst rund um die Uhr (24/7) umfassend überwacht werden muss und ob Personal für zeitnahe Reaktionen bei Angriffen bzw. Sicherheitsvorfällen vorgehalten werden muss.

Zur Nachvollziehbarkeit der Administration, der Zugriffe auf die Daten durch Mitarbeiter sowie zur Erkennung von Angriffen sollten Protokolldateien (z. B. über Systemstatus, fehlgeschlagene Authentisierungsversuche etc.) und weitere sicherheitsrelevante Datenquellen wie z. B. Auswertungen von Tools zur Systemüberwachung (IDS, IPS, Data Leakage Prevention etc.) herangezogen und korreliert werden. Alle relevanten Protokolldaten, die sich auf Finanzdaten beziehen, müssen revisionssicher gespeichert werden.

5 Notfallmanagement

Der vorbeugende Schutz gegen mögliche Gefährdungen ist eine wichtige Aufgabe bei den Bemühungen um Sicherheit. Die Erfahrung zeigt aber, dass gravierende Störungen und Unglücke auch bei bester Vorsorge nicht vollständig verhindert werden können. Und oftmals sind es unverhoffte Ereignisse, welche die größten Risiken mit sich bringen, scheinbar lokal begrenzte Ereignisse entwickeln oft unerwartete Breitenwirkungen.

Um gegen solche Vorfälle gewappnet zu sein und um angemessen auf Notfallsituationen reagieren zu können, sollte daher jeder eCommerce-Anbieter über ein funktionierendes Notfallmanagement (Business Continuity Management) verfügen, basierend auf etablierten Standards. Dazu gehört es, entsprechende organisatorische Strukturen aufzubauen sowie Konzepte zu entwickeln, die eine rasche Reaktion bei auftretenden Notfällen und die rasche Wiederaufnahme zumindest der wichtigsten Geschäftsprozesse ermöglichen.

Um die Wirksamkeit von Maßnahmen im Bereich des Notfallmanagements zu überprüfen, sollten regelmäßig Tests und Notfallübungen durchgeführt werden.

6 Sicherheitsprüfung und -nachweis

Ein Bestandteil jedes erfolgreichen Informationssicherheitsmanagements ist die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheits-Prozesses. eCommerce-Anbieter müssen regelmäßig den IT-Sicherheitszustand ihrer Geschäftsprozesse, Dienste und ihrer Plattformen überprüfen und kontinuierlich verbessern und weiterentwickeln. Hierzu sollten regelmäßig Informationssicherheitsrevisionen (IS-Revisionen) und IT-Penetrationstests durch unabhängige Dritte durchgeführt werden.

Um die Wirksamkeit vorhandener technischer Sicherheitsmaßnahmen zu überprüfen, sind toolbasierte Netzscans und Penetrationstests ein erprobtes und geeignetes Vorgehen. Sie dienen dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System sowohl durch interne als auch durch externe Angreifer vorab einzuschätzen und daraus notwendige ergänzende Sicherheitsmaßnahmen abzuleiten. eCommerce-Anbieter sollten für die von ihnen betriebenen Netze, Systeme und Anwendungen vor Inbetriebnahme und regelmäßig im laufenden Betrieb toolbasierte Netzscans und Penetrationstests durchführen.

Nutzt ein eCommerce-Anbieter Subunternehmen zur Erbringung seiner Services, so entbindet ihn dies nicht von der Verpflichtung, die Sicherheit dieser Dienste zu überprüfen.

Generell müssen alle Formen von Sicherheitsprüfungen von Personen mit geeigneten Qualifikationen durchgeführt werden. Diese dürfen jedoch nicht an der Erstellung der geprüften Strategien und Konzepte beteiligt gewesen sein, um Betriebsblindheit und Konflikte zu vermeiden. Die Prüfer bzw. Auditoren müssen möglichst unabhängig und neutral sein.

7 Personal

Informationssicherheit wird unmittelbar von den Personen getragen, die mit den jeweiligen Informationen umgehen.

7.1 Anforderungen an das Personal

Es ist essentiell, dass das beim eCommerce-Anbieter tätige Personal (intern und extern) ausreichend eingearbeitet und zu allen eingesetzten Techniken ebenso geschult wird wie zu Informationssicherheit und Datenschutz. Personen, die sicherheitsrelevante Aufgaben ausüben wie Administratoren und Mitarbeiter mit Zugang zu finanzwirksamen oder vertraulichen Informationen, müssen vertrauenswürdig und zuverlässig sein.

Die Aufgabenverteilung und die hierfür erforderlichen Rollen sind so zu strukturieren, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu minimieren oder ganz auszuschalten. Ein rollenbasiertes Rechtemanagement, das nur Zugriff auf diejenigen Daten und Systeme zulässt, die zur Erfüllung der jeweiligen Aufgaben notwendig sind, bietet hier die notwendige organisatorische und technische Unterstützung.

Alle Personen, die Zugang zu Kundendaten haben, sind in besonderem Maße über ihre Pflichten im Umgang mit diesen hinzuweisen. Auch bei Subunternehmen sollte auf die Auswahl und den Wissensstand des Personals geachtet werden.

Das Personal ist über die bestehenden Regelungen und Handlungsanweisungen zur Informationssicherheit, zum Datenschutz sowie zum Umgang mit Kundendaten zu unterrichten und auf deren Einhaltung nachweislich zu verpflichten.

7.2 Schulungen

Auch im Bereich eCommerce werden viele neue Techniken und IT-Komponenten eingesetzt. Die Innovations- und Updatezyklen sind daher in diesem Bereich sehr kurz. Deshalb sind die Mitarbeiter regelmäßig so zu schulen, dass sie alle eingesetzten Techniken, Komponenten und Funktionalitäten beherrschen. Die Mitarbeiter müssen aber auch alle Sicherheitsimplikationen rund um diese Techniken kennen und im Griff haben.

Da Fehlkonfigurationen in einer eCommerce-Umgebung gravierende Folgen für die darauf bereitgestellten Ressourcen haben können, erhöhen sich die Anforderungen an die Administratoren. Daher ist es wichtig, dass die Administratoren ausreichende Kenntnisse über die eingesetzten Produkte und zugrunde liegenden Techniken besitzen, damit sie Probleme aus

eigenem Handeln heraus vermeiden, technische Probleme rechtzeitig erkennen und beseitigen sowie die Funktionen und Sicherheitsmerkmale der zugrunde liegenden Technologien optimal nutzen können. Sie müssen insbesondere in der Lage sein, die Folgen von Konfigurationsänderungen abschätzen zu können.

Damit sichergestellt ist, dass die Administratoren auch über aktuelle Sicherheitsrisiken informiert sind, sollte der eCommerce-Anbieter dafür sorgen, dass sie über aktuelle CERT-Meldungen verfügen und sich regelmäßig weiterbilden können.

Alle Mitarbeiter müssen außerdem kontinuierlich für generelle Informationssicherheits- und Datenschutzbelange sensibilisiert werden.

7.3 Personalausstattung

Die Praxis zeigt es, dass erfolgreiche Angriffe meist auf fehlerhaft konfigurierte, ungepatchte oder unzureichend überwachte Systeme zurückzuführen sind. Die Ursache dafür liegt oftmals in einer nicht ausreichenden Personalausstattung im Bereich IT-Betrieb, IT-Administration und Informationssicherheit. Eine ausreichende Personalausstattung ist daher sicherzustellen.

8 Datenschutz

In eCommerce-Systemen werden grundsätzlich immer personenbezogene Daten erhoben, verarbeitet, gespeichert und genutzt. Daher muss der Schutz personenbezogener Daten gemäß den datenschutzrechtlichen Bestimmungen gewährleistet sein.

9 Konkretisierende Standards

- BSI Standards zur Internetsicherheit (ISi-Reihe)
  http://www.isi-reihe.de
- Payment Card Industry Data Security Standard (PCI-DSS)
  https://www.pcisecuritystandards.org/security_standards/index.php
- aktueller Algorithmenkatalog der Bundesnetzagentur (BNetzA)
  http://www.bundesnetzagentur.de/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html
- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS),
  https://www.bsi.bund.de/grundschutz/standards
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise,
  https://www.bsi.bund.de/grundschutz/standards
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz,
  https://www.bsi.bund.de/grundschutz/standards
- BSI-Standard 100-4: Notfallmanagement,
  https://www.bsi.bund.de/grundschutz/standards
- ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems requirements specification", ISO/IEC JTC1/SC27
- ISO/IEC 27002:2005 "Information technology - Code of practice for information security management", ISO/IEC JTC1/SC27
- ISF: The Standard of Good Practice for Information Security,
  https://www.isfsecuritystandard.com