Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Management von Schwachstellen und Sicherheitsupdates

Empfehlungen für kleine Unternehmen und Selbstständige

1 Ausgangslage

Aufgrund der großen Komplexität heutiger Software sind Fehler bei der Entwicklung nicht zu vermeiden. Moderne Entwicklungsprozesse unterstützen zwar gezielt bei der Programmierung sicherer Software, trotzdem treten Schwachstellen nach wie vor häufig auf. Diese Fehler müssen nicht immer unmittelbar sicherheitskritische Folgen haben, Schutzmechanismen im Betriebssystem oder in der Anwendung selbst verhindern oftmals eine schadhafte Ausnutzung. In der Praxis ist dennoch ein entsprechendes Management von Schwachstellen und Sicherheitsupdates durch den Anwender erforderlich: Die Gefährdungslage sollte permanent abgeschätzt und verfügbare Sicherheitsupdates kurzfristig ausgerollt werden. Bis diese Sicherheitsupdates verfügbar sind, müssen wirksame Maßnahmen gegen die Ausnutzung offener Schwachstellen ergriffen werden.

2 Ziel

Die vorliegende BSI-Veröffentlichung zur Cyber-Sicherheit bietet Hinweise und Hilfestellungen zum Management von Schwachstellen und Sicherheitsupdates in kleinen Unternehmen und für Selbstständige. In solchen Umgebungen sind Produkte zur zentralisierten Verwaltung der IT-Systeme oftmals nicht im Einsatz. Es werden im Folgenden ausschließlich Schwachstellen in Softwareprodukten betrachtet, die durch Fehler bei der Entwicklung der Software entstanden sind und nicht solche, die bei der Verwendung der Software etwa auf schlechte organisatorische Prozesse oder eine fehlerhafte Konfiguration zurückzuführen sind.

Betrachtet werden die folgenden Phasen:

- Bewertung der Gefährdungslage
- Ergreifen von Gegenmaßnahmen
- Management von Sicherheitsupdates und deren Ausrollung

Beachten Sie zusätzlich auch das Dokument BSI-CS 027 „Lebenszyklus einer Schwachstelle“[1], ebenfalls aus der Reihe „BSI-Veröffentlichungen zur Cyber-Sicherheit“.

3 Bewertung der Gefährdungslage

Für ein wirksames Management von Schwachstellen und Sicherheitsupdates müssen zu jedem Zeitpunkt die folgenden Fragen beantwortet werden können:

- Welche Softwareprodukte werden eingesetzt?
- Weisen die eingesetzten Softwareprodukte bekannte offene Schwachstellen auf?
- Wie ist der Grad der aus diesen offenen Schwachstellen resultierenden Gefährdungslage?

1 https://www.allianz-fuer-cybersicherheit.de/dok/6643430

3.1 Welche Softwareprodukte werden eingesetzt?

Eine möglichst einheitliche IT-Umgebung erleichtert die Kontrolle über installierte Softwareprodukte. Nur Administratoren sollten dazu berechtigt sein, selbstständig Anwendungen zu installieren, da sonst die Kontrolle über vorhandene Programme und deren Versionsstände verloren geht.

Beschränken Sie die Anzahl der verwendeten Softwareprodukte auf das notwendige Minimum, um die Angriffsfläche zu reduzieren. Erstellen Sie eine Übersicht aller eingesetzten Produkte und gewichten Sie diese nach dem möglichen Gefährdungspotenzial. Einer hohen Gefährdung ausgesetzt sind auf Client-Systemen üblicherweise das Betriebssystem selbst, Web-Browser und Büro-Anwendungen, mit denen auch Daten aus fremden Quellen verarbeitet werden. Ebenfalls gefährdet sind Serverdienste jeglicher Art, etwa Web-Server oder File-Server. Dies gilt insbesondere, wenn diese einen Zugriff von außerhalb ermöglichen. Eine zusätzliche Gefährdung geht dabei von Systemen aus, die für mehrere Zwecke eingesetzt werden – ein Arzt sollte z. B. prüfen, ob ein Rechner neben dem Zugriff auf die Patientendatenbank auch für normales Web-Surfen genutzt wird; dadurch entstehen ebenso unnötige wie inakzeptable Einfallstore für Schadsoftware.

Außerdem sollten Sie die Bedeutung der Verfügbarkeit einer Anwendung für Ihr Unternehmen bewerten: Ist das Produkt für die tägliche Arbeit essenziell oder im Zweifel für einen gewissen Zeitraum verzichtbar? Eine wichtige Rolle spielt in diesem Zusammenhang die Identifikation besonders schützenswerter Daten. Das Gefährdungspotenzial ist umso höher, je schützenswerter die mit dem jeweiligen Softwareprodukt verarbeiteten Daten sind. Hier können insbesondere auch gesetzliche Anforderungen eine Rolle spielen.

Ab einer größeren Anzahl von zu verwaltenden Systemen empfiehlt sich der Einsatz einer Lösung zur Software-Inventarisierung. Diese sind oftmals in Produkten zur zentralisierten Software-Installation enthalten.

3.2 Weisen die eingesetzten Softwareprodukte bekannte offene Schwachstellen auf?

Prüfen Sie regelmäßig, ob für die von Ihnen eingesetzten Softwareprodukte neue Schwachstellen bekannt geworden sind. Folgende Quellen sind dabei empfehlenswert:

- Sicherheitshinweise des jeweiligen Herstellers – viele Hersteller bieten z. B. entsprechende Mailinglisten oder RSS-Feeds an
- Informationsangebote des BSI – hierzu gehören die Kurzmeldungen von CERT-Bund[2] und das Bürger-CERT[3] sowie die Schwachstellenampel[4]
- Informationsangebote und Warndienste von IT-Sicherheitsdienstleistern
- Nachrichten und Warndienste von IT-Fachpresse und IT-Informationsdiensten

Achten Sie außerdem auf Meldungen über auslaufenden Support für bestimmte Softwareprodukte oder Produktversionen, um frühzeitig Alternativen planen zu können.

3.3 Wie ist der Grad der aus diesen offenen Schwachstellen resultierenden Gefährdungslage?

Üblicherweise enthalten die Meldungen zu neuen Schwachstellen eine Einschätzung zur Schwere der Lücke und der daraus entstehenden Gefährdungen. Unterschiedliche Quellen verwenden verschiedene Verfahren, um diese Einschätzung durchzuführen. Dabei spielen eine Reihe von Faktoren eine Rolle, etwa die Art der Ausnutzung (von „nur lokal“ bis hin zu „aus der Ferne“, d. h. über das Internet), das Resultat der Ausnutzung (von „Programmabsturz“ bis hin zu

2 https://www.cert-bund.de
3 https://www.buerger-cert.de
4 https://www.cert-bund.de/schwachstellenampel

„Code-Ausführung mit Systemrechten“) oder die Verfügbarkeit von Möglichkeiten zur Ausnutzung (von „nur der Hersteller hat Kenntnis“ bis hin zu „Metasploit-Modul verfügbar“) sowie von Gegenmaßnahmen.

Allgemein und herstellerübergreifend etabliert hat sich das Common Vulnerability Scoring System (CVSS)[5]. Eine höhere Punktzahl („Score“) bedeutet eine höhere Gefährdungslage. Unter Nutzung des erstellten Verzeichnisses eingesetzter Softwareprodukte sollte die eigene Betroffenheit geprüft werden und zumindest bei Schwachstellen mit einer höheren Gefährdungslage eine Einzelfallprüfung aller bekannten Informationen über diese Schwachstelle erfolgen. Beachten Sie dabei auch Ihre eigene Gewichtung des Gefährdungspotenzials und der Verfügbarkeit der Anwendung sowie die Wichtigkeit der damit verarbeiteten Daten.

4 Ergreifen von Gegenmaßnahmen

Basierend auf der im vorigen Kapitel beschriebenen Bewertung der Gefährdungslage müssen im Fall des Auftretens einer Schwachstelle geeignete Gegenmaßnahmen getroffen werden. Auch diese sind, wie im Folgenden beschrieben, auf Notwendigkeit, Wirksamkeit und Praktikabilität zu prüfen.

4.1 Keine Gegenmaßnahmen

Im einfachsten Fall ist die Gefährdungslage so gering, dass es ausreicht, die Verfügbarkeit eines Sicherheitsupdates abzuwarten.

4.2 Vorläufige Gegenmaßnahmen (Mitigations)

In vielen Fällen empfehlen entweder der Hersteller des betroffenen Produkts oder Dritte hilfsweise vorläufige Gegenmaßnahmen, oftmals auch als Mitigations bezeichnet. Diese können von einer Umkonfiguration des Produkts über Deaktivierung von einzelnen Bestandteilen bis hin zu provisorischen Vorab-Fixes reichen. Mitigations sollten nach einer Prüfung umgehend umgesetzt werden, wenn dadurch die Gefährdungslage reduziert werden kann. Es ist darauf zu achten, ob und in welcher Form eine Mitigation nach Verfügbarkeit eines Sicherheitsupdates wieder rückgängig gemacht werden muss.

4.3 Eigene Gegenmaßnahmen

Stellt der Hersteller selbst keine unmittelbaren Gegenmaßnahmen bereit, können unter Umständen eigene getroffen werden. Hierzu gehören beispielsweise eine Zugriffsbeschränkung für betroffene Dienste (z. B. Zugriffsmöglichkeiten nur noch aus dem Intranet bzw. über VPN), striktere Firewall-Regelungen, der Einsatz von oder eine Erweiterung bestehender Paketfilter oder Monitoring-Tools sowie der Einsatz generischer Mitigation-Tools.

4.4 Produktverzicht

Im schlimmsten Fall ist es aufgrund einer akuten Gefährdungslage nicht mehr vertretbar, ein Produkt überhaupt weiter einzusetzen. In diesem Fall sollten Alternativprodukte zur Verfügung stehen. Beispielsweise hat sich im Bereich der Web-Browser die sogenannte Zwei-Browser-Strategie bewährt, bei der von einem aktuell angreifbaren Browser ohne Zeitverzug temporär auf einen anderen gewechselt werden kann. Allerdings ist diese Strategie etwa bei Spezialsoftware oder komplexen Diensten mit zahlreichen Abhängigkeiten kaum möglich oder praktikabel. Sie sollte jedoch stets auch im Hinblick auf auslaufenden Produktsupport berücksichtigt werden, wobei hier üblicherweise eine größere Vorlaufzeit für einen Wechsel auf ein Alternativprodukt besteht.

5 https://www.first.org/cvss/user-guide

5 Management von Sicherheitsupdates und deren Ausrollung

Im Regelfall stellt der Hersteller eines Softwareprodukts ein Sicherheitsupdate zur Verfügung, um eine aufgetretene Schwachstelle zu beheben. Seinen Zweck erfüllt ein Sicherheitsupdate jedoch erst dann vollständig, wenn es tatsächlich durchgängig auf allen betroffenen Systemen installiert wurde.

5.1 Grundsätzliche Überlegungen

Idealerweise sollte eine IT-Infrastruktur möglichst einheitlich sein und zentral verwaltet werden. Wie oben geschildert, erleichtert dies die Inventarisierung der zu berücksichtigenden Softwareprodukte. Gleichzeitig können über zentralisierte Lösungen auch Sicherheitsupdates bzw. aktualisierte Programme gezielt und mehrstufig ausgerollt werden. Zahlreiche Hersteller bieten entsprechende Lösungen an, deren Einsatz ab einer größeren Anzahl von zu verwaltenden Systemen dringend empfohlen wird. Bezüglich des Einsatzes ist abzuwägen, ob der Aufwand des Betriebs einer solchen Lösung geringer ist als der sonst nötige manuelle Aufwand zur Pflege der eigenen IT-Systeme. Oftmals sind auch entsprechende Dienste bereits Bestandteil der Betriebssysteme bestimmter Hersteller. Bekannte Vertreter sind hier z. B. Microsofts Windows Server Update Services (WSUS) als Komponente von Microsoft Windows Server oder das für Ubuntu verfügbare Landscape. In einer zentral verwalteten IT-Umgebung sollten alle direkt in die Anwendungen integrierten Aktualisierungsfunktionen abgeschaltet und jegliche Aktualisierungen nur zentral gesteuert durchgeführt werden.

In sehr kleinen IT-Umgebungen oder gar bei Einzelplatzrechnern ist eine zentrale Verwaltung üblicherweise nicht praktikabel. Ein strukturiertes Konzept zum Management von Sicherheitsupdates ist dann umso wichtiger. In diesen Fällen ist insbesondere der Einsatz von vollautomatischen, durch den jeweiligen Hersteller in seine Anwendungen integrierten Update-Mechanismen zu prüfen. Für solche Szenarien sollen im Folgenden konkrete Hinweise gegeben werden.

5.2 Vorbereitungen

Basierend auf der durchgeführten Inventarisierung der verwendeten Softwareprodukte können diese in drei Klassen eingeteilt werden:

- Software, die eine integrierte vollautomatische Installation von Updates ermöglicht
- Software mit integrierter Aktualisierungsfunktion, welche jedoch vom Anwender ausgeführt werden muss
- Software ohne Aktualisierungsfunktion

In sehr kleinen IT-Umgebungen und auf Einzelplatzrechnern stellen vollautomatische Updates sicher, dass die jeweiligen Softwareprodukte stets auf dem neuesten Stand sind. Eine Verwendung ist daher grundsätzlich zu empfehlen. Der Sicherheitsgewinn durch vollautomatische Updates für das Betriebssystem und geläufige Anwendungsprogramme überwiegt insbesondere dann deutlich, wenn Aktualisierungen sonst nicht zeitnah oder gar nicht eingespielt würden.

Zu beachten ist jedoch stets, dass eine neue Programmversion unter Umständen Kompatibilitätsprobleme verursachen oder Funktionen verlieren kann. Als besonders kritisch oder unverzichtbar bewertete Softwareprodukte sollten daher von vollautomatischen Updates ausgenommen werden. Dies ermöglicht ein kontrolliertes Vorgehen bei der Aktualisierung und schützt vor bösen Überraschungen. Idealerweise kann eine solche Aktualisierung zunächst auf einem Testsystem geprüft werden.

Für Software, die nur eine manuelle oder gar keine Aktualisierungsfunktion beinhaltet, sollten Sie sich regelmäßige Erinnerungen einrichten, sodass eine manuelle Prüfung auf Updates erfolgen kann. Auch hier sollten Aktualisierungen für kritische Software zunächst auf einem Testsystem installiert und geprüft werden.

Um im Ernstfall gewappnet zu sein, sollten regelmäßige Backups selbstverständlich sein – auch ein vom Hersteller gut getestetes Update kann in Einzelfällen zu Systemausfällen führen.

5.3 Im Ernstfall

Ist ein Produkt von einer Schwachstelle betroffen, empfiehlt sich die Durchführung der folgenden Schritte:

1. Sobald Sie feststellen, dass ein verwendetes Softwareprodukt von einer Schwachstelle betroffen ist, sollten Sie nach Bewertung der resultierenden Gefährdungslage zunächst, wie oben beschrieben, geeignete Gegenmaßnahmen in die Wege leiten.
2. Anschließend muss regelmäßig geprüft werden, ob bereits ein Sicherheitsupdate verfügbar ist. Neben den oben genannten Quellen für Information über Schwachstellen können hier ebenfalls die integrierten Aktualisierungsfunktionen genutzt werden.

Abhängig davon, ob das betroffene Produkt vollautomatische Aktualisierungen verwendet oder nicht, muss nun eine Unterscheidung erfolgen.

5.3.1 Variante A: Vollautomatische Updates werden verwendet

3. Sobald ein Update verfügbar ist, wird es ohne manuelles Zutun durch den automatischen Update-Mechanismus installiert. Prüfen Sie dennoch zeitnah, ob die Aktualisierung erfolgreich war.
4. Prüfen Sie , ob eventuelle vorab angewendete vorläufige Gegenmaßnahmen (Mitigations) rückgängig gemacht werden müssen und schalten Sie diese – wenn erforderlich – wieder ab.

5.3.2 Variante B: Vollautomatische Updates sind nicht verfügbar oder bewusst abgeschaltet

3. Sobald ein Sicherheitsupdate verfügbar ist, sollte es nach Möglichkeit zunächst geprüft und getestet werden. Installieren Sie den Patch zunächst nur auf einem Rechner oder idealerweise auf einem dedizierten Testsystem und verifizieren Sie, dass es keine Probleme gibt.
4. Installieren Sie den Patch möglichst zeitnah auf allen betroffenen Systemen und schalten Sie dann – wenn erforderlich – die getroffenen vorläufigen Gegenmaßnahmen (Mitigations) wieder ab.

6 Beispielhafte Tabelle zum Management von Schwachstellen und Sicherheitsupdates

Die nachfolgende Tabelle zeigt exemplarisch, wie die in den vorherigen Kapitel beschriebenen Aspekte für die eigene IT-Umgebung strukturiert festgehalten und gepflegt werden können. Sie kann als Grundlage für die Durchführung eines manuellen Managements von Schwachstellen und Sicherheitsupdates in kleinen IT-Umgebungen dienen.

Name	Version	Gefährdungspotenzial	Wichtigkeit	Offene Schwachstellen?	Gefährdung	Sicherheitsupdate verfügbar	Sicherheitsupdate eingespielt	Mitigation	letzte Prüfung	Anmerkungen
TextEditor	1.31	niedrig	niedrig	nein	-	-			17.11.2013	-
Browser A	31	hoch	hoch	ja	hoch	nein	nein	Browser B nutzen	18.11.2013	CVE 2013-xxxx, Remote Code Execution mit Benutzerrechten
LogoDesign	3.4	niedrig	hoch	ja	niedrig	ja	nein		18.11.2013	CVE-2013-xxxx, Programmabsturz

Tabelle 1: Exemplarische Tabelle als Grundlage für die Durchführung eines manuellen Managements von Schwachstellen und Sicherheitsupdates