HOCHSCHULE OSNABRÜCK
UNIVERSITY OF APPLIED SCIENCES

Richtlinie zum IT-Schwachstellenmanagement

Inhaltsverzeichnis

1. Inhalt und Ziel dieser Richtlinie

Diese Richtlinie beschreibt Maßnahmen und Regelungen mit dem Ziel, Schwachstellen in IT-Systemen der Hochschule zeitnah zu identifizieren und zu beheben. Diese Maßnahmen und Regelungen werden unter dem Begriff Software Vulnerability Management (SVM) zusammengefasst. Übergeordnetes Ziel ist der Schutz der Hochschule vor Angriffen aus dem Internet, insbesondere Ransomware-Angriffen.

Zahlreiche Universitäten und Hochschulen sind inzwischen Opfer von Ransomware-Angriffen geworden. Bei einem solchen Angriff breitet sich eine Schadsoftware zunächst im internen Netzwerk aus. Nach der Ausbreitungsphase erfolgt dann eine Datenabzug- und/oder Verschlüsselungsphase mit anschließender Erpressung.

Um solche Angriffe zu vermeiden ist es wichtig, insbesondere Server, die über das Internet erreichbar sind, sicher zu betreiben. Um bei einem eventuellen Befall eines Systems mit Schadsoftware die weitere interne Ausbreitung möglichst weit einzuschränken, ist es auch wichtig, Systeme, die nicht über das Internet erreichbar sind, möglichst sicher zu konfigurieren und auf einem aktuellen Stand zu halten. Dies betrifft sowohl Clients (z.B. Arbeitsplatz-PCs) als auch Server. Im Vergleich zu Clients sind Server jedoch gefährdeter, da sie Dienste anbieten und i.d.R. permanent laufen. Clientsysteme sind vor Zugriffen durch eine sogenannte Endpoint-Firewall geschützt, wie in der „Richtlinie IT-Sicherheit und Datenschutz der Hochschule Osnabrück“ gefordert.

Es ist geplant, die vorliegende Richtlinie nach einem Jahr auf Grundlage der bis dahin gewonnenen Erfahrungen zu prüfen und ggf. zu aktualisieren.

2. Geltungsbereich und gesetzliche Grundlagen

Diese Richtlinie gilt für sämtliche IT-Systeme im Netz der Hochschule Osnabrück, also sämtliche über eine IP-Adresse erreichbaren IT-Systeme. Sie richtet sich an Systemverantwortliche / Administrator*innen, die diese Systeme betreiben.

3. Allgemein Regeln

3.1. Benennung von Systemverantwortlichen für sämtliche Systeme

Für jedes System am Netzwerk der Hochschule ist eine Systemverantwortliche bzw. ein Systemverantwortlicher zu benennen. Systemverantwortliche müssen Mitarbeiter*innen der Hochschule sein (keine Studierenden). Zur Identifizierung der Systeme werden eindeutige IP-Adressen verwendet.

3.2. Das ITSC führt eine Liste der Systeme und Systemverant-wortlichen

Um bei identifizierten Schwachstellen dezentraler IT-Systeme umgehend zugehörige Systemverantwortliche ansprechen zu können, führt das ITSC eine Liste der Systemverantwortlichen. Aktuelle Dokumentationsform der Liste ist das IP-Adressmanagement (IPAM).

4. Aufgaben des IT Service Centers

4.1. Regelmäßige Schwachstellenscans

Das ITSC führt mindestens vierteljährlich einen systematischen Schwachstellen-Scan über das gesamte Hochschulnetz durch. Daneben werden bedarfsorientiert, z.B. bei erhöhter Risikolage, zusätzliche Scans durchgeführt. Die Ergebnisse des Scans werden dokumentiert. Die Dokumentation wird so ausgeführt, dass ein Vergleich mit Ergebnissen vorhergehender Scans möglich ist.

4.2. Umgehende Benachrichtigung von Systemverantwortlichen

Bei Identifizierung sicherheitskritischer Schwachstellen (Klassifizierung „rot“ und „gelb“) von Systemen informiert das ITSC umgehend die zugehörigen

Systemverantwortlichen und stellt diesen das zugehörige Ergebnis des Schwachstellen-Scans bereit.

Bei Nicht-Erreichbarkeit der oder des Systemverantwortlichen informiert das ITSC den dezentralen bzw. die dezentrale SVM[1]-Admin (s. Abschnitt 6) der Organisationseinheit.

4.3. Reaktion bei sicherheitskritischen Schwachstellen

Die im Regelfall verwendeten Fristen zum Abstellen der identifizierten Schwachstellen sind nachstehend angegeben.

Scanergebnis	Erreichbarkeit	Frist zur Behebung
rot	Über das Internet	Sofortige Sperrung der externen Erreichbarkeit
gelb	Über das Internet	2 Wochen
rot	Nur intern	1 Monat
gelb	Nur intern	2 Monate

Für über das Internet erreichbare Server wird die Erreichbarkeit über das Internet nach Fristablauf durch das ITSC unterbunden. Die Sperrung wird im Regelfall erst dann wieder aufgehoben, wenn ein erneuter (gezielter) Scan zeigt, dass die Schwachstellen behoben wurden.

Für interne, nicht über das Internet erreichbare Systeme kann das ITSC nach Fristablauf den Netzzugang blockieren.

Aufgrund besonderer, durch das BSI mitgeteilter Bedrohungslagen, können die Fristen durch das ITSC angepasst werden.

5. Aufgaben von Systemverantwortlichen

5.1. Aufrechterhaltung der IT-Sicherheit des Systems

Systemverantwortliche sind für den sicheren Betrieb ihrer Systeme zuständig.

Hierunter fallen u.a. folgende Aufgaben:

- Software auf einem aktuellen Stand halten, insbesondere zeitnahes Einspielen von Security-Patches.
- Virenscanning
- Schutz des Systems durch eine Endpoint-Firewall
- Nutzer*innen- und Berechtigungsmanagement für das System

Systemverantwortliche sollten im Rahmen der Inbetriebnahme eines neuen Systems einen Schwachstellen-Scan des Systems durchführen bzw. über ihre bzw. ihren dezentralen SVM-Admin veranlassen.

[1] Software Vulnerability Management

Vor der Freigabe der Internet-Erreichbarkeit eines Servers ist durch einen Schwachstellen-Scan zu verifizieren, dass der Server keine relevanten Schwachstellen aufweist.

5.2. Meldung von Zuständigkeitsänderungen an das ITSC

Personelle Änderungen der Zuständigkeit sind umgehend an das ITSC zu melden, damit dem ITSC stets die aktuellen Systemverantwortlichen bekannt sind.

6. Dezentrale SVM-Admins

Jede Fakultät / dezentrale Organisationseinheit benennt ein bis zwei SVM-Admins.

Die SVM-Admins erhalten Zugang zum Vulnerability-Scanner der Hochschule und werden so geschult, dass sie Scans durchführen und zugehörige Scan-Ergebnisse / Reports abrufen können.

Aufgabe der SVM-Admins ist es, für Systemverantwortliche einzelne Systeme zu scannen und den Systemverantwortlichen die Scan-Ergebnisse zu übermitteln.

Hierdurch sollen die SVM-Admins einen Überblick über die Risikolage ihrer Organisationseinheit gewinnen und bei deren Beurteilung unterstützen.

7. Eskalation bei erforderlichem Weiterbetrieb

In der Regel sollten identifizierte Schwachstellen durch Security-Patches zeitnah behoben werden können.

Eine Abweichung vom Regelfall ist dann gegeben, wenn Systeme trotz kritischer Schwachstellen („rot“ oder „gelb“) über die festgelegte Frist hinaus weiter betrieben werden sollen.

Mögliche Fälle[2]:

- Einsatz eingekaufter Produkte, die durch den Hersteller nicht hinreichend gewartet werden.

  Für dauerhaft eingesetzte Software-Produkte sollen im Regelfall Wartungsverträge abgeschlossen werden, die eine regelmäßige zeitnahe Aktualisierung der Software durch den Hersteller im Fall identifizierter Schwachstellen sicherstellen.
- Patches können aufgrund von Abhängigkeiten zwischen Komponenten ggf. nicht eingespielt werden.
- Einsatz interner Systeme, für die kritische Schwachstellen identifiziert wurden, die jedoch nicht behoben werden können, aufgrund z.B. fehlender Patches.

In einem solchen Fall sind die Risiken eines Weiterbetriebs gegenüber den Funktionalitätseinschränkungen einer Außerbetriebnahme bzw. Sperrung abzuwägen.

Hierfür wird der folgende **Eskalationsprozess** vorgesehen:

[2] Der Einsatz unsicherer studentischer Systeme in der Lehre („Spielwiese“) wird nachstehend separat behandelt

Schritt 1: Detaillierung der Risikobewertung

Beteiligte: Systemverantwortende, Mitarbeiter*in des IT-Sicherheitsteams des ITSC, ggf. Fachbereichsleiter*in ITSC.

Bei den Scan-Ergebnissen handelt es sich um allgemeine Risikobewertungen, die den spezifischen Einsatz und Schutzbedarf des Systems nicht berücksichtigen. Eine genaue Risikobeurteilung kann daher nur in Zusammenarbeit zwischen der bzw. dem Systemverantwortlichen, welche bzw. welcher die fachliche Einsatzweise des Systems kennt, und dem IT-Sicherheitsteam des ITSC, das Erfahrung mit der spezifischen Risikobeurteilung hat, erfolgen.

Z.B. kann es sein, dass ein System durch eine Schwachstelle, die die Vertraulichkeit gefährdet, auf „rot“ steht, das System jedoch nur einen geringen Schutzbedarf hinsichtlich Vertraulichkeit aufweist und das resultierende Risiko daher akzeptabel ist.

Die CVSS[3]-Bewertung sieht hierfür speziell eine Risikobewertung abhängig von der Einsatzumgebung und Schutzbedarfsanforderungen vor, die über die allgemeine Risikobewertung hinaus geht.

Auch kann es sein, dass das Risiko durch Zusatzmaßnahmen außerhalb des Systems in einfacher Weise reduziert werden kann.

Ergebnisalternativen:

1. Weiterbetrieb tragbar, da das Risiko als akzeptabel eingeordnet wurde.
2. Weiterbetrieb mit festgelegten Zusatzmaßnahmen möglich => Zusatzmaßnahmen dokumentieren (z.B. VPN-Zugang statt Internet-Freigabe von Diensten)
3. Risiko bleibt hoch, Weiterbetrieb stellt hohes Risiko dar

Das Ergebnis ist zusammen mit einer Begründung und ggf. erforderlichen Zusatzmaßnahmen zu dokumentieren.

Schritt 2: Abwägung Nutzen gegenüber Risiken eines Weiterbetriebs

Nur notwendig, wenn der Weiterbetrieb ein hohes Risiko darstellt.

Zusätzliche Beteiligte: ITSC-Leitung/Fachbereichsleitung, Bedarfsträger (z.B. Professoren), ggf. IT-Sicherheitsbeauftragte/r

Aufgabe: Abwägung der Risiken eines Weiterbetriebs gegenüber den Funktionalitätseinschränkungen einer Außerbetriebnahme bzw. Sperrung.

Ergebnisalternativen:

1. Begründete Empfehlung eines Weiterbetriebs, ggf. mit Zusatzmaßnahmen
2. Begründete Empfehlung eine Außerbetriebnahme bzw. Internet-Sperrung

Das Ergebnis ist zusammen mit den ggf. erforderlichen Zusatzmaßnahmen zu dokumentieren.

[3] Common Vulnerability Scoring System, System zur standardisierten Risikobewertung von Schwachstellen

Schritt 3: Entscheidung

Nur notwendig, wenn Weiterbetrieb in Schritt 2 empfohlen wurde.

Zusätzliche Beteiligte: Zuständige/r Vizepräsident*in (CIO), IT-Sicherheitsbeauftragte/r

Ergebnisalternativen:

- Entscheidung gemäß oder gegen Empfehlung. Die Entscheidung ist zu dokumentieren.

8. Umgang mit studentischen Systemen in der Lehre

Betroffen ist insbesondere die Lehre in Informatik-Bereichen, bei denen Studierende spezielle Server (z.B. WebServer, Datenbank-Server) zu Übungszwecken aufsetzen oder IoT-Komponenten konfigurieren und es dabei aus Aufwandsgründen nicht leistbar ist, die Systeme gleichzeitig durchgängig abzusichern.

Für den Betrieb solcher „Übungssysteme“ gelten folgende Regeln:

1. Die Übungssysteme sind dem ITSC zu melden und es ist eine bzw. ein Verantwortliche/r anzugeben, die bzw. der im Bedarfsfall Systeme deaktivieren kann.
2. Die Übungssysteme dürfen nicht über das Internet erreichbar sein.
   (Unsicher konfigurierte Systeme mit Schwachstellen können über das Internet automatisiert erkannt, angegriffen und kompromittiert werden.)

   Falls ein Zugriff auf die Übungssysteme über das Internet erforderlich ist, sind hierzu mit dem ITSC abgestimmte Verfahren zu nutzen (z.B. VPN).
3. Die Übungssysteme sind in einem separaten Teilnetz zu betreiben, von dem kein direkter Zugriff auf andere Hochschulnetze möglich ist.

   Der Zugriff auf das Internet wird für die Übungssysteme nicht gesperrt. Über das Internet können daher Hochschuldienste von diesen Systemen (wie von jedem externen System) aus verwendet werden.

   Werden weitergehende Zugriffsmöglichkeiten gefordert, sind diese explizit mit dem ITSC abzustimmen und vom ITSC freizugeben (Dokumentation!).
4. Übungssysteme sollen nach Möglichkeit in virtuellen Umgebungen betrieben werden, die vom ITSC bereitgestellt werden.