Amtliche Bekanntmachung der Fachhochschule Südwestfalen

- Verkündungsblatt der Fachhochschule Südwestfalen -

Baarstraße 6, 58636 Iserlohn

Nr. 1345 Ausgabe und Tag der Veröffentlichung: 20.03.2025

Richtlinie der Fachhochschule Südwestfalen
zum Umgang mit nicht behobenen Schwachstellen
von extern administrierten Systemen im Hochschulnetz
vom 18.03.2025

Das Rektorat der Fachhochschule Südwestfalen hat in seiner Sitzung am 05.03.2025 die Richtlinie der Fachhochschule Südwestfalen zum Umgang mit nicht behobenen Schwachstellen von extern administrierten Systemen im Hochschulnetz verabschiedet.

Der Wortlaut wird im Folgenden bekannt gegeben:

Hinweis:
Nach Ablauf eines Jahres nach Bekanntmachung dieser Ordnung können nur unter den Voraussetzungen des § 12 Absatz 5 Hochschulgesetz NRW Verletzungen von Verfahrens- oder Formvorschriften des Hochschulgesetzes oder des Ordnungs- oder des sonstigen Rechts der Hochschule geltend gemacht werden, ansonsten ist eine solche Rüge ausgeschlossen.

Richtlinie der Fachhochschule Südwestfalen zum Umgang mit nicht behobenen Schwachstellen von extern administrierten Systemen im Hochschulnetz

Inhaltsverzeichnis

Vorwort

Mit dieser Richtlinie soll sichergestellt werden, dass die IT-Sicherheit innerhalb des Hochschulnetzes auch bei extern administrierten Systemen gewahrt bleibt und im Falle von Schwachstellen angemessene und rechtzeitige Maßnahmen ergriffen werden. Die Richtlinie wird aufgrund des Projekts SOC-Hochschulen.nrw eingeführt. Das Schwachstellen-Scanning ist ein Service des Security Operations Centers, welcher durch die Zusammenarbeit mit dem Managed Security Services Provider "DATAGROUP" monatlich durchgeführt wird. Unter „extern administrierten Systemen“ werden alle Systeme verstanden, die im IP-Adressbereich der Fachhochschule Südwestfalen liegen und nicht von IT-Services verwaltet werden. Die Richtlinie bezieht sich nicht auf die Geräte von Endanwendern (Clients), sondern ausschließlich auf Systeme (z. B. Server, virtuelle Server, NAS usw.), die kontinuierliche Dienste bereitstellen (z. B. Webanwendungen, Schnittstellen, Datenbanken usw.)

1. Zielsetzung

Diese Richtlinie regelt den Umgang mit nicht behobenen Schwachstellen, die in extern administrierten Systemen innerhalb des Hochschulnetzes identifiziert wurden und die nicht von der Hochschulverwaltung (IT-Services) administriert werden. Ziel ist es, die IT-Sicherheit der Hochschule zu gewährleisten und Risiken durch nicht behobene Schwachstellen zu minimieren.

2. Geltungsbereich

Die Richtlinie gilt für alle extern administrierten Systeme innerhalb des Hochschulnetzes, die von außen erreichbar sind und nicht von IT-Services administriert werden. Hierzu zählen insbesondere die Systeme der einzelnen Fachbereiche, Forschungs- und Lehreinrichtungen sowie anderer Organisationseinheiten der Hochschule, die im Netzwerk der Hochschule betrieben werden.

3. Identifikation und Meldung von Schwachstellen

Sollte eine kritische Schwachstelle im Rahmen des Schwachstellen-Scannings in einem externen System festgestellt werden, wird diese unverzüglich per E-Mail an den zuständigen Betreiber / Fachbereich des Systems gemeldet. Die Meldung erfolgt durch den ISB. Der zuständige Betreiber / Fachbereich wird, sofern möglich, im Vorfeld von IT-Services ermittelt. Die Schwachstelle wird detailliert beschrieben, und gegebenenfalls werden erste Handlungsempfehlungen zur Behebung bereitgestellt. Ist der Betreiber nicht ermittelbar, wird die zuständige Stelle benachrichtigt, die über die Zuweisung des IP-Adressbereichs identifiziert wird.

4. Behebung der Schwachstellen durch den Betreiber

Der Betreiber des betroffenen Systems ist verpflichtet, die gemeldete Schwachstelle innerhalb von 4 Wochen nach Erhalt der Meldung zu beheben, jedoch spätestens bis zum nächsten Schwachstellen-Scanning. Dies gilt sowohl für Schwachstellen, die durch externe Bedrohungen als auch für solche, die durch interne Sicherheitslücken bedingt sind.

5. Konsequenzen bei nicht behobenen Schwachstellen

Wird die Schwachstelle bis zu dem darauffolgenden Schwachstellen-Scanning nicht behoben, erfolgt eine Nachverfolgung sowie die Festlegung erforderlicher Maßnahmen durch den Informationssicherheits-beauftragten. Die Umsetzung der Maßnahmen erfolgt durch IT-Services. Diese Maßnahmen können die Einschränkung der Erreichbarkeit des betroffenen Systems im Hochschulnetz bis hin zur vollständigen Abschaltung des Systems umfassen, sofern dies zur Wahrung der IT-Sicherheit erforderlich ist.

6. Durchsetzung von Sicherheitsmaßnahmen

IT-Services ist berechtigt, geeignete Sicherheitsmaßnahmen zu ergreifen, um die Integrität und Sicherheit des Hochschulnetzes zu gewährleisten. Diese Maßnahmen können, je nach Schweregrad der Schwachstelle, die temporäre oder permanente Einschränkung des Zugriffs auf das betroffene System bis hin zur vollständigen Abschaltung umfassen. Die Einschränkungen werden nach einer Risikobewertung festgelegt und in Abstimmung mit IT-Services umgesetzt. Der Betreiber wird über die Maßnahmen informiert und bleibt so lange eingeschränkt, bis die Schwachstelle behoben wurde.

7. Dokumentation und Reporting

Alle identifizierten Schwachstellen, die durch externe Systeme verursacht werden, sowie die durchgeführten Maßnahmen werden im Ticketsystem dokumentiert. Der Informationssicherheitsbeauftragte berichtet regelmäßig über den Status der Schwachstellenbehebung an die Hochschulleitung und informiert die betroffenen Stellen.

8. Ausnahmefälle und Eskalation

Falls es aus bestimmten Gründen nicht möglich ist, die Schwachstelle innerhalb des vorgegebenen Zeitrahmens zu beheben, muss der Betreiber einen schriftlichen Antrag auf Verlängerung der Frist an den Informationssicherheitsbeauftragten stellen. Dieser wird im Einzelfall geprüft. Bei schwerwiegenden oder wiederkehrenden Sicherheitsvorfällen kann die Angelegenheit an eine höhere Instanz eskaliert werden, die über das weitere Vorgehen entscheidet.

9. Richtlinie des Rektorats

Diese Richtlinie tritt am Tag nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Fachhochschule Südwestfalen in Kraft. Ausgefertigt aufgrund des Beschlusses des Rektorats vom 05.03.2025. Die Richtlinie wird nach Ablauf von zwei Jahren überprüft und ggf. angepasst.

Iserlohn, 18.03.2025

Der Rektor der Fachhochschule Südwestfalen

Prof. Dr. Dr. Dr. habil. Alexander Prange