Die Hochschule Anhalt unterhält ein Programm zur Aus- und Weiterbildung der Mitarbeitenden und Professorinnen und Professoren zu den Themen Informationssicherheit und Datenschutz, welches vom ISI-Schulungsteam durchgeführt wird.

Folgende Veranstaltungen werden angeboten:

Studierendenkurs (deutsch/englisch)
IT-Vorkurs- und Basisschulung
weiterführender Mittelstufenkurs
Expertenkurs (überwiegend für Administratoren)
Workshops
Games (Escape Room, Ransomware)
Phishing Simulationen zu Trainingszwecken
Live Security Events

Haben Sie schon Ihr Zertifikat?

Aufgrund des gestiegenen Sicherheitsbedarfs an der Hochschule Anhalt und auch zu Ihrem persönlichen Schutz empfehlen wir Ihnen die Teilnahme an einer der angebotenen Schulungen passend zu Ihrem individuellen Kenntnisstand.

Folgende Inhalte werden mit unterschiedlichem Detaillierungsgrad vermittelt:

IT-Begriffe und grundsätzliche Absicherung gegen Angriffe (Passwortsicherheit, Schutz vor Phishing, Malware und im Netz, Datenschutz und -umgang)
Verhalten beim Informationssicherheitsvorfall
Angriffserkennung und -verhinderung

Nach erfolgreicher Absolvierung erhalten Sie das jeweilige Informationssicherheitszertifikat, das Sie dem Personaldezernat als Ergänzung Ihrer Qualifizierungen in der Personalakte weiterleiten können.

KONTAKT

HOCHSCHULE ANHALT University of Applied Sciences

Hochschule Anhalt
University of Applied Sciences
Bernburger Straße 55
06366 Köthen

Wir freuen uns über Ihre Teilnahme und Ihr Feedback zu unseren Schulungen!

Kontakt

Informationssicherheit (ISI) der Hochschule Anhalt

Informationssicherheitsbeauftragte/r

Telefon: +49 (0) 3496 67 5415
isi@hs-anhalt.de
Notfall-Telefon: 5500

Unter folgendem Link erhalten Sie u.a. aktuelle Informationen, weitere Sicherheitstipps und die Möglichkeit zur Einsicht, wann welche Schulungen durchgeführt werden:

www.hs-anhalt.de
/isi-schulungen

HOCHSCHULE ANHALT University of Applied Sciences

„TheShadow“

Escape Game der ISI-Mittelstufe

Bild: Izabella Jasper | Pixabay

Das ISI-Schulungsteam informiert über den Mittelstufenkurs für Informationssicherheit & Datenschutz

Stand: 08/2024 | ISI-Team

www.hs-anhalt.de
/informationssicherheit

Kernthemen

der ISI-Mittelstufe

Im Mittelstufenkurs der Schulungsreihe „Informationssicherheit und Datenschutz“ des ISI-Schulungsteams werden in einem online Kurs, der mit einem spannenden Live Escape Game um die Person „The Shadow“ kombiniert ist, die folgenden Kernthemen der Informationssicherheit behandelt. Durch die Zuordnung der einzelnen Kapitel zum sog. MITRE ATT&CK Framework kann der Ablauf eines Cyberangriffs in seinen jeweiligen Stufen nachvollzogen werden. Warum diese fünf Kernthemen für unsere Hochschule so wichtig sind, erfahren Sie in diesem Flyer und ausführlicher im Mittelstufenkurs.

MITRE ATT&CK Framework & OSINT

Das MITRE ATT&CK Framework ist eine allgemein zugängliche Wissensbasis. In ihr werden Angriffstaktiken und -techniken aufgezählt, welche Cyberkriminelle verwenden, um ihre Ziele zu erreichen. **Projektverantwortliche, die sich bei der Beschaffung und Absicherung ihrer IT auf die gängigen Angriffstechniken konzentrieren, können frühzeitig, aktuelle Bedarfe erkennen und sich leichter Prioritäten setzen.**

Neben dem MITRE ATT&CK Framework gibt es ein weiteres, öffentlich verfügbares Framework, welches ebenfalls der Informationsbeschaffung dient: das OSINT-Framework. Es bietet in strukturierter Form eine Datenbank für öffentliche Tools zur Datenanalyse. Verschiedene Werkzeuge innerhalb des Frameworks ermöglichen eine effektive Datenerfassung aus verschiedenen Online-Quellen, einschließlich sozialer Medien und Suchmaschinen. Sie erstrecken sich auch auf die Erforschung des Deep und Dark Web und bieten Einblicke in verschiedene Sektoren. **Personen und Organisationen, die weniger Informationen in öffentlich verfügbaren Quellen zur Verfügung stellen, erschweren den Angreifern die Erstellung eines exakten Profils und verringern damit ihre Angriffsfläche.**

Social Engineering

Menschen sind soziale Wesen und benötigen den Austausch und die Interaktion mit Menschen. Beim Social Engineering machen sich Angreifer dieses tief verwurzelte, menschliche Bedürfnis zunutze. Allerdings gehen sie dabei nicht ehrlich, sondern trickreich vor. Sie täuschen eine Identität oder eine Situation vor und fordern ihr Gegenüber zum Handeln auf. Oft sind es die menschlichen Schwächen, die das Opfer bewusst, aber in falschem Glauben oder unbewusst tätig werden lassen.

Menschen, die sich ihrer Schwächen, aber auch ihrer Verantwortung in Bezug auf die Geheimhaltung von Organisationsinformationen bewusst sind, lassen sich bei entsprechender Schulung nicht so einfach von vorgespielten Szenarien täuschen und vereiteln somit geplante Social Engineering-Angriffe auf die schützenswerten Daten der Organisation.

Ransomware

Malware wird von Cyberkriminellen selbst programmiert oder sie wird gekauft oder als Dienstleistung zum Kauf im Dark Web angeboten. Ransomware ist die Art von Schadsoftware, welche zur Verschlüsselung von Dateien und ganzen Systemen verwendet wird und die Erpressung von Lösegeld zum Ziel hat. Es gibt Vereinigungen, die auf Webseiten durch die Zurverfügungstellung von Entschlüsselungstools gegen die Verbreitung von Ransomware kämpfen oder die sich darauf spezialisiert haben, mit den Angreifertruppen über die Höhe des Lösegelds zu verhandeln.

Organisationen, die ihre Daten durch ein zentrales Backup sichern, das getrennt von den anderen Systemen des IT-Netzes lagert und bei Bedarf problemlos wieder eingespielt werden kann, entziehen den Cyberkriminellen die Grundlage für ihr Ransomware-Geschäftsmodell.

Netzwerk

Für die Übertragung von Informationen zwischen Kommunikationspartnern werden Netzwerkkomponenten und darauf abgestimmte Kommunikationsprotokolle benötigt. Zusammen regeln sie, in welcher Form und wohin die Informationen fließen. Cyberkriminelle nutzen z. B. Verwundbarkeiten in Protokollen, Fehler und Schwachstellen in Systemkonfigurationen oder hochprivilegierte Nutzerkonten für ihre Angriffe auf das Netzwerk aus. Abwehrtechnologien im Netzwerkbereich reichen von der Nutzerauthentifizierung, über die Einbruchserkennung und -vorbeugung, das Schwachstellen-Management bis hin zum Monitoring von Prozessen.

Organisationen, welche das Zero-Trust-Prinzip „never trust, always verify“ in den fünf Säulen Identitäten, Geräte, Netzwerke, Anwendungen und Daten abgebildet haben, machen es sowohl Innentätern als auch Angreifern von außen extrem schwer, ihre Angriffe durchzuführen.

Verschlüsselung

Mit zunehmender Rechenleistung durch Quantencomputer wird es zukünftig auch Angreifern gelingen, schwache Verschlüsselungen zu berechnen und somit zu knacken. Für Organisationen ist es dann wichtig, ihre für den jeweiligen Anwendungsfall gewählten Verschlüsselungsverfahren hinsichtlich ihrer Sicherheit zu prüfen. Das betrifft die Verschlüsselung von Daten während der Authentifizierung, der Verarbeitung, des Transports und während der Speicherung.

Organisationen, die ihre gewählten Verschlüsselungsverfahren kontinuierlich anpassen und aktualisieren, werden gegen fortschrittliche Angriffsmethoden auch in Zukunft bestehen können.