

Security Awareness Kampagne

| | |
|--------------------------|--|
| Themenbereiche: | Security / Privacy |
| Studierender: | Andri Widmer |
| Betreuungsperson: | Björn Näf |
| Experte: | Gian-Luca Frei |
| Auftraggebende: | Verein Kooperative Speicherbibliothek Schweiz |
| Keywords: | IT-Sicherheit, Awareness, CIS, Security, Privacy |

1. Aufgabenstellung

Um die IT-Sicherheit des Vereins kooperative Speicherbibliothek Schweiz (VKSS) zu erhöhen, soll eine massgeschneiderte Security Awareness Kampagne geplant, vorbereitet und initial umgesetzt werden. Benötigte Unterlagen für die Schulungen sowie für die Tests sollen erarbeitet und anhand eines Zeitplans zur Verfügung gestellt werden. Die Konzipierung der Kampagne soll sich dabei an den Empfehlungen des Critical Security Controls (CIS), genauer Control 14, orientieren.

2. Lösungskonzept

Die Methodik der Bachelorarbeit wurde bereits im Vorfeld durch den Auftraggeber definiert. Es handelt sich dabei um das CIS Framework. Im Control 14 von CIS befinden sich neun Schutzmassnahmen, die zur Erstellung einer Security Awareness Kampagne umgesetzt werden sollen. Diese neun Schutzmassnahmen lauten wie folgt:

- Einrichtung und Aufrechterhaltung eines Programms zur Förderung des Sicherheitsbewusstseins
Schulung der Mitarbeiter
- zur Erkennung von Social-Engineering-Angriffen
- in bewährten Authentifizierungsverfahren
- zu bewährten Praktiken im Umgang mit Daten
- zu den Ursachen für unbeabsichtigte Datenexposition
- zur Erkennung und Meldung von Sicherheitsvorfällen
- wie sie fehlende Sicherheitsupdates für ihre Unternehmensressourcen erkennen und melden können
- über die Gefahren der Verbindung und Übertragung von Unternehmensdaten über unsichere Netzwerke
- in rollenspezifischen Schulungen zum Sicherheitsbewusstsein und zu den Sicherheitsfähigkeiten

Diese neun Schutzmassnahmen wurden in folgende Themenbereiche für die Schulungen unterteilt: Social Engineering, Authentifizierung, Datenverarbeitung, Datenexposition, Sicherheitsvorfälle, Updates und unsichere Netzwerke. Anhand einer Literaturrecherche wurden die verschiedenen Themenbereiche aufgearbeitet und die Theorie für die Erstellung der Schulungsunterlagen zusammengetragen. In einem weiteren Schritt wurden nach einer Diskussion mit den Ansprechpersonen der Speicherbibliothek und der Ermittlung des Umfangs der Themenbereiche verschiedene Schulungskanäle für die einzelnen Themenbereiche festgelegt.

| | PowerPoint | Video | Blogpost | Plakate | Forms | Phishing Simulation |
|---------------------|------------|-------|----------|---------|-------|---------------------|
| Social Engineering | X | | | | X | X |
| Authentifizierung | X | X | | | X | |
| Datenverarbeitung | | | X | | X | |
| Datenexposition | | | | X | X | |
| Sicherheitsvorfälle | | | X | | X | |
| Updates | X | | | | X | |
| Unsichere Netzwerke | | | X | | X | |

Wie aus der Tabelle ersichtlich wird, werden die Kanäle PowerPoint, Video, Blogpost, Plakate, Forms und Phishing Simulation verwendet. Nachdem festgelegt wurde, welche Kanäle für welche Themengebiete verwendet werden, wurde ein Zeitplan erstellt.

| Bereich/Monat | Januar | Februar | März | April | Mai | Juni | Juli | August | September | Oktober | November | Dezember |
|---------------------|--------|---------|------|-------|-----|------|------|--------|-----------|---------|----------|----------|
| Authentifizierung | | | | | | | | | | | | |
| Datenverarbeitung | | | | | | | | | | | | |
| Datenexposition | | | | | | | | | | | | |
| Sicherheitsvorfälle | | | | | | | | | | | | |
| Updates | | | | | | | | | | | | |
| Unsichere Netzwerke | | | | | | | | | | | | |
| Social Engineering | | | | | | | | | | | | |

Aus der Abbildung wird ersichtlich, dass die Dauer eines Schulungsblocks ungefähr einen Monat beträgt. Dieser Zeitblock umfasst die Präsentation des Themas oder das Selbststudium der zur Verfügung gestellten Materialien, die Absolvierung des Onlinetests sowie dessen Nachbesprechung. Durch die Verteilung der einzelnen Schulungsblöcke über das Jahr in Abständen von zwei Monaten soll gewährleistet werden, dass sich die Mitarbeiter stetig mit dem Thema IT-Sicherheit befassen müssen.

3. Spezielle Herausforderungen

Die Einschränkung, dass bereits ein Framework mit vorgegebenen Schutzmassnahmen für die Erstellung der Kampagne vorgegeben war, definierte die Themenbereiche und Ziele, welche die Security Awareness Kampagne beinhaltet. Daraus resultierten vor allem am Anfang Probleme bei der Literaturrecherche, welche die entsprechenden Schutzmassnahmen abdecken.

4. Ergebnisse

Das Ergebnis der Bachelorarbeit ist ein Schulungskonzept mit Schutzmassnahmen aus dem CIS Control 14, welches die erarbeiteten Themenbereiche, unterschiedliche Schulungskanäle sowie einen Zeitplan für die

einzelnen Schulungen enthält. Zudem wurden Schulungsunterlagen für jeden Themenbereich, sowie Onlinetests für die Messung des Erfolges erstellt.

5. Ausblick

Der Auftrag umfasste eine initiale Schulung einer der definierten Schutzmassnahmen. Aufgrund der zeitlichen Begrenzung der Bachelorarbeit finden die weiteren Schulungen der Schutzmassnahmen nach deren Abgabe statt. Die Ergebnisse der Onlinetests der kommenden Schulungen sind noch abzuwarten und deren Analyse wäre interessant. Diese Ergebnisse könnten einerseits verwendet werden, um die Security Awareness Kampagne für die kommenden Jahre anzupassen und den Lernerfolg der Mitarbeiter zu maximieren. Andererseits könnte anhand der Resultate abgeleitet werden, bei welchen Themengebieten Handlungsbedarf besteht und eine Nachschulung erforderlich ist.

Bei mehrfach wiederholter Durchführung der Kampagne sollte ebenfalls eruiert werden, inwiefern der vermittelte Lernstoff der Themenbereiche bei den Mitarbeitern noch präsent ist. Dies um zu erkennen, wie die Security Awareness durch die Kampagne stetig gesteigert werden kann.