Security as a Service

Modus: Einzelarbeit in Gruppen

Typ: Miniproject

Beschreibung

In diesem Miniproject beschäftigen Sie sich intensiv mit den Möglichkeiten und Problemen, die durch unachtsame Nutzung von Technologien entstehen können. Sie finden mögliche Angriffsvektoren bei einer Ihnen bekannten Person und geben als Expert_in möglichst konkrete Empfehlungen, Tipps und Vorschläge. Zusätzlich entwickeln Sie für diese Person einen Notfall-Guide der im Falle einer erfolgten Attacke rasch und einfach nutzbar ist.

Ablauf

Führen Sie während des gesamten Prozesses ein Forschungstagebuch (siehe Beschreibung im Anhang). Dokumentieren Sie darin die Aktivitäten, Ergebnisse, Hindernisse und Erfolge sämtlicher Schritte Ihrer Arbeit.

1. Wählen Sie einen Freund oder eine Freundin aus, die kein_e Informatiker_in ist, aber trotzdem regelmäßig Technologien nutzt. Je unterschiedlicher und interessanter das Nutzungsverhalten, desto spannender wird auch Ihr Miniprojekt ausfallen.

Diese Person sollte auch mit den Details Ihres Projektes vertraut gemacht werden, und zustimmen, alle notwendigen Informationen zur Verfügung zu stellen.

2. Führen Sie mit dieser Person ein Gespräch, bei dem Sie im Detail die Nutzung von verschiedenen Technologien wie Cloud Lösungen, Remote Zugriffe, Passwortdatenbanken, Zweifaktor Authentifizierung, Backups, Email-Verhalten, Email-Client, verwendeter Browser, etc. erfragen.

Informieren Sie sich als Vorbereitung über dieses Gespräch über gängige Sicherheitsprobleme. Nutzen Sie die folgende Liste von Links, um sich ein wenig einzulesen:

- https://internethealthreport.org/2018/die-geschichte-eines-ransomware-opfers/?lang=de
- https://www.wired.co.uk/article/ransomware-attack-recovery-hackney
- https://www.onlinesicherheit.gv.at/Themen/Gefahren-im-Netz/Privatsphaere/Identitaetsdiebstahl.html
- https://bundeskriminalamt.at/202/Internet_kennen/
- https://cyberrisk-rating.at/cyberrisk-2024-schema-de.pdf
- https://www.aura.com/learn/dangers-of-identity-theft
- https://allaboutcookies.org/consequences-of-identity-theft

Versuchen Sie, im Gespräch ausreichend notwendige Details in Erfahrung zu bringen um der Person Empfehlungen, Tipps und Vorschläge geben zu können. Auch konkrete Gerätehersteller und Modelle können zu Angriffsvektoren werden.

3. Verfassen Sie ein ausführliches Risikoprofil der Person in Form einer Matrix. Zuerst identifizieren Sie alle Risiken, also beispielsweise Angriffsformen, Ausfälle, Verlust, etc., die auf Grund der Technologienutzung entstehen werden. Diese werden auf der senkrechten Achse der Matrix eingetragen.

Die Matrix hat dann vier weitere Spalten:

- die Wahrscheinlichkeit, dass so ein Problem auftritt
- die Höhe des Schadens beim Eintreten des Problems
- wie schnell reagiert werden müsste, wenn dieses Problem auftritt (im wesentlichen: wie wichtig ist das betroffene Gerät/Service/etc.)
- wie aufwändig die Behebung wäre

	Wahrscheinlichkeit	Schadenshöhe	Reaktion	Aufwand
Befall mit Ransomware	niedrig	hoch	schnell	sehr groß
Datendiebstahl	sehr niedrig	mittel	keine	keiner
Festplattenschaden	hoch	sehr hoch	schnell	sehr groß
Telefon verloren	mittel	mittel	sehr schnell	mittel

Die Werte in der Matrix sind nur grobe Schätzungen; es genügt also eine einfache Skala mit wenigen Schritten, also beispielsweise [sehr niedrig | niedrig | mittel | hoch | sehr hoch].

Stimmen Sie dieses Risikoprofil mit der Person ab.

3. Recherchieren Sie im Internet zu allen Problemen mit hoher Verletzlichkeit (siehe Slidebook Criminal Thinking) bzw. hoher Dringlichkeit der Behebung nach Vorschlägen, wie für Durchschnittsnutzer_innen solche Problem vermeiden oder verhindern können, oder sich auf das Eintreten vorbereiten (zB. regelmäßige Backups).

Dokumentieren Sie, welchen Fragen Sie nachgegangen sind, wie Sie gesucht haben, welche Quellen Sie gefunden haben, und woraus Sie schließen, dass diese Vorschläge auch für die Person zutreffen sind! Beschreiben Sie jeweils Maßnahmen, die jetzt (also punktuell) und/oder ab jetzt regelmäßig ergriffen werden sollten, und wie die Reaktion auf das Eintreten des Problems aussehen sollte.

4. Sie entwickeln jetzt aus all diesen Informationen eine Security-Fibel, also ein kleines Handbuch zugeschnitten auf die Bedürfnisse der Person, mit der Sie hier arbeiten. Das Handbuch soll das Risikoprofil Schritt für Schritt durchgehen, und für jedes Problem beschreiben, ob oder wie Vorkehrungen zu treffen sind und wie die beste Reaktion auf das Eintreten des jeweiligen Problems aussieht. Versuchen Sie, Ihre Vorschläge so konkret und umsetzbar wie möglich zu halten.

Schreiben Sie das Handbuch in einfacher Sprache und vermeiden oder erklären Sie Fachbegriffe.

5. Schreiben Sie weiters einen Emergency Guide, der konkrete, einfache und auch in Stresssituationen leicht zu folgende Handlungsempfehlungen enthält. Dieser Emergency Guide sollte Teil der Security-Fibel sein und extra übersichtlich gestaltet werden. Die Security-Fibel ist Teil Ihrer Abgabe.

6. Präsentieren und besprechen Sie Ihre Arbeit mit der Person. Erfragen Sie gezielt, welche Handlungsempfehlungen sinnvoll wirken und welche zu viel Aufwand für die Person selbst bedeuten. Dokumentieren und reflektieren Sie, was Sie beim nächsten Mal optimieren und verbessern können, aber auch, was gut angenommen wurde.

Bonus: helfen Sie der Person bei der Umsetzung Ihrer Vorschläge (zB. Einrichtung eines regelmäßigen Backups) und erzählen Sie uns davon.

Abgabe

7. Ihre Abgabe besteht aus Ihrem Forschungstagebuch, eventuell bereinigt um persönliche Einträge, die Sie nicht preisgeben wollen, sowie den Teilen, die oben als Teile der Abgabe genannt sind. Gliedern Sie dieses Dokument bitte sinnvoll, und bemühen Sie sich, ein gut lesbares Layout zu gestalten. Erzeugen Sie dann daraus ein PDF[1] und geben Sie dieses im entsprechenden Abschnitt in TUWEL ab.

Bitte beachten Sie, dass Aufgaben dieses Typs **nach spätestens 2 Wochen abgegeben** werden müssen (ab der Verfügbarkeit dieser Beschreibung), und dann noch eine Review-Phase (1 Woche) durchlaufen. **Ihr selbst gewählter Termin gilt erst für die Endabgabe!**

Zusatz für Endabgabe

Ein wesentlicher Teil Ihrer Endabgabe ist der Abschnitt *Reflexion & Feedback*. Beantworten Sie dabei die folgenden Fragen für die finale Abgabe, also nachdem Sie die Reviews geschrieben/bekommen haben, und ergänzen Sie Ihr PDF um einen entsprechenden Abschnitt:

- Wie wurde Ihr Verständnis der gewählten Denkweise durch diese Übungsarbeit verändert?
- Glauben Sie, ein nachhaltiges Verständnis der gewählten Denkweise wird Ihnen im Studium oder danach im Beruf helfen?
- Welche Teile dieser Arbeit fanden Sie besonders schwer, welche zu einfach?
- Welche Aspekte dieser Arbeit haben Ihnen gut gefallen, welche würden Sie ändern?
- Was haben Sie bei dieser Arbeit gelernt? Ist diese Art von Übungsformat Ihrer Meinung nach sinnvoll?
- Hat das Schreiben der Reviews geholfen, Ihre eigene Arbeit zu verbessern? Falls ja: wie?
- Haben die Reviews, die sie bekommen haben geholfen, Ihre eigene Arbeit zu verbessern? Falls ja: wie?
- Sind Sie mit Ihrer Arbeit zufrieden?

Beachten Sie: Die Antworten auf die Fragen im Abschnitt *Reflexion und Feedback* gehen **nicht** in die Beurteilung Ihrer Arbeit ein!

Beachten Sie bitte die Richtlinie zur Verwendung von generativer AI, die im PDF »Denkweisen der Informatik 2023« zu finden ist. Wesentliche Teile der Arbeit dürfen nicht durch generative AI-Systeme verfasst werden!

---

[1] Beachten Sie bitte, dass inzwischen alle aktuellen Betriebssysteme die Erzeugung von PDFs ohne zusätzliche Software erlauben. Geben Sie keine PDFs ab, bei denen Werbung oder Wasserzeichen von Gratis-Software eingebettet ist. Für Unterstützung befragen Sie bitte die allwissende Müllhalde (das Internet) bzw. https://www.wikihow.com/Convert-a-File-Into-PDF

Anhang: Forschungstagebuch

Ein Forschungstagebuch ist ein (physisches oder digitales) Medium, in dem Sie den Fortschritt Ihrer Arbeit und Ihre Gedanken dazu bzw. Probleme damit schriftlich festhalten. Damit Ihr Forschungstagebuch dabei helfen kann, zufällige Ideen oder plötzliche Inspirationen notieren können, sollten Sie es immer bei sich haben (das spricht stark für ein digitales Forschungstagebuch). Für die Zwecke dieser Arbeit genügt eine einfache Text-Datei. Jeder Eintrag ist mit Datum und Uhrzeit versehen.

Einträge im Forschungstagebuch werden zB. zu folgenden Anlässen gemacht:

- Artikel gelesen (mit kurzer Anmerkung der Relevanz für Ihr Thema, Auflistung für SIe wesentlicher Punkte)
- Gute Suchbegriffe für Ihr Thema
- In einem Gespräch etwas relevantes gehört, mit Ideen, wie Sie das weiterverfolgen könnten
- Teil der Arbeit geschrieben, mit Einschätzung der Qualität

Sie können auch persönliche Dinge im Forschungstagebuch festhalten, also erfreuliche (zB. Gute Quelle gefunden!) wie unerfreuliche (zB. heute gar nichts weitergegangen, sehr frustrierend). Für die Abgabe des Forschungstagebuchs können Sie Teile, die Sie nicht preisgeben wollen, entfernen.

Anhang: Qualität von Quellen

Ein wesentlicher Teil der Recheche im Internet ist die Einschätzung der Qualität von Quellen. Dazu gibt es, nicht ganz unironisch, viele Hilfestellungen im Internet. Wir haben einige davon für Sie zusammengestellt, denen wir vertrauen:

- Saferinternet, Quellen richtig beurteilen – https://www.saferinternet.at/news-detail/online-quellen-richtig-beurteilen-aber-wie
- Lehrerfortbildung Baden-Württemberg, Arbeitstechnik 2: Überprüfung von Quellen im Internet – https://lehrerfortbildung-bw.de/u_gewi/gk/gym/bp2016/fb5/2_komp/6_vorlagen/3_methode/02_technik2/
- Wer es ganz genau will: Qualitätskriterien für wissenschaftliches Arbeiten – https://soztheo.de/forschung/qualitaetskriterien-fuer-wissenschaftliches-arbeiten/

Anhang: wie man einen wissenschaftlichen Artikel liest

Wissenschaftliche Artikel sind meistens nicht dafür geschrieben, von vorne bis hinten gelesen zu werden. In Ihrem Studium werden Sie aber viele wiss. Publikationen lesen. Da hilft es oft, eine klare Strategie zu haben, wie man das angeht.

Ich habe hier für Sie die Ultrakurzversion zusammengeschrieben. Sie finden nach diesem kurzen Guide einige Links zu längeren Versionen. Dieser Guide gilt für »typische« wissenschaftliche Texte, also solche, die dem üblichen Aufbau folgen.

1. Überfliegen Sie das Abstract. Sie werden dann verstehen, um was es im Artikel geht, warum die Arbeit verfasst wurde, und in wenigen Worten üblicherweise auch, was das Ergebnis der Arbeit war. Das hilft Ihnen, den Rest besser einordnen zu können.

2. Lesen Sie jetzt den letzten Abschnitt des Papers, üblicherweise »Conclusions« oder »Discussion« genannt. Damit sollten Sie jetzt wissen, was die Autor_innen gemacht haben, und warum Sie es gemacht haben. Sie wissen auch, was dabei herausgekommen ist.

3. Der Abschnitt vor den Schlussfolgerungen sind üblicherweise »Results«. Überfliegen Sie diesen Teil, um zu sehen, wie relevant er für Sie ist.

4. Sehen Sie sich die Abbildungen an. In groben Zügen können Sie jetzt verstehen, um was es in diesem Paper geht, und was die Autor_innen gemacht haben. Zugegeben, das wird einfacher, je öfter Sie es machen.

5. Es sollte einen Abschnitt geben, der die Methodologie beschreibt, meistens »Methods« o.ä. Versuchen Sie grob zu verstehen, wie die Autor_innen gearbeitet haben (qualitativ, quantitativ, etc.).

Sie haben jetzt ein gutes Bild davon, um was es geht, und können entscheiden, ob Sie den Rest des Papers auch lesen wollen (zB. weil es relevant oder interessant ist). Eventuell ist aber auch nur noch der Abschnitt »Related Work« (o.ä.) für Sie spannend, weil Sie dort weitere Papers finden, die sich mit derselben oder einer ähnlichen Fragestellung beschäftigen – und vielleicht suchen Sie ja genau solche Arbeiten.

Weitere Guides:

- https://drewdennis.medium.com/how-to-read-scientific-papers-quickly-efficiently-e7030c4018fa
- https://www.bmj.com/about-bmj/resources-readers/publications/how-read-paper
- https://paperpile.com/g/read-scientific-paper/