# Not-so-zero-day-anymore

**Modus:** Einzelarbeit

**Typ:** Guided Research

### Beschreibung

Für diese Arbeit recherchieren Sie eine ausreichend interessante *Zero-Day Vulnerability*, die mindestens 5 Jahre alt ist und zu der Sie ausreichend Informationen finden. Dokumentieren Sie möglichst viele Fakten rund um den Ursprung der Schwachstelle, also nicht nur betroffene Systeme, Datum der Entdeckung und Reaktion seitens der betroffenen Herstellerfirma, sondern auch (falls auffindbar) Entstehung, eventuelle Exploits und deren Reichweite, Schäden etc. Wesentlich in Ihrer Dokumentation ist das Datum der Behebung sowie die eventuellen Folgen, wenn die Schwachstelle beispielsweise zur Verbreitung einer spezifischen Schadsoftware genutzt wurde, die natürlich mit der Behebung der Schwachstelle nicht plötzlich verschwunden 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. Informieren Sie sich darüber, was eine Zero-Day Vulnerability ist. Lesen Sie auf Wikipedia und mindestens einer anderen Seite, wie der Begriff definiert ist, und formulieren Sie Ihre eigene Definition. Dokumentieren Sie den Prozess im Forschungstagebuch.

2. Sehen Sie sich diese Liste von aktuellen Zero-Day Vulnerabilities durch:

https://www.securin.io/zero-days-list/

Überlegen Sie, von welchen dieser Schwachstellen Sie selbst akut betroffen sind, weil Sie Produkte oder Services verwenden, die Sie auf dieser Liste finden.

3. Suchen Sie nach einer Vulnerability, die vor mindestens 5 Jahren noch ein »Zero-Day« war. Ein guter Suchbegriff für solche alten Zero-Days ist *famous zero-day vulnerabilities.* Suchen Sie sich eine alte Zero-Day Vulnerability aus und fertigen Sie einen Steckbrief an: Wann war das, was war betroffen, was war die Verletzlichkeit, was konnte man damit machen etc.

4. Recherchieren Sie dann etwas detaillierter so gut es geht die folgenden Informationen:

- Wann und wie wurde der Zero-Day bekannt?
- Wie lange vor dem Bekanntwerten war die Vulnerability schon vorhanden?
- Wie viele Geräte/Serviceinstanzen waren zum Zeitpunkt der Veröffentlichung betroffen?
- Wie hat die für den Zero-Day verantwortliche Instanz (Hersteller, Betreiber, OSS-Community, etc.) reagiert?

- Warum gab es die Zero-Day Vulnerability? Gibt es Dokumentation dazu, wie die Schwachstelle entstanden ist?
- Wie schnell wurde eine Behebung bereitgestellt?
- Wie schnell hat sich diese Behebung verbreitet?
- Welche dokumentierten Expoits dieser Schwachstelle gibt es? Von welcher Malware wurde die Schwachstelle genutzt?
- Welche Schäden wurden durch die Schwachstelle vermutlich verursacht?
- Wie gut wurde die Schwachstelle behoben, dh. eine Einschätzung davon, in wieviele der betroffenen Instanzen/Geräte die Behebung tatsächlich eingespielt/installiert wurde.

Hinweis: Sie werden vermutlich nicht zu allen diesen Fragen gleich ausführliche Antworten finden.

5. Versuchen Sie, mittels der Security-Suchmaschine shodan.io herauszufinden, wieviel verletzliche Instanzen der betroffenen Geräte bzw. Services es heute noch gibt. Beachten Sie bitte, dass es dazu nicht genügt, den Namen des Zero-Day in shodan einzugeben; suchen Sie also nach einem entsprechenden Suchbegriff, der Ihnen die Zahl verletzlicher Geräte zeigt.

### Abgabe

6. 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 spätestens **2 Wochen nach der Verfügbarkeit** dieser Beschreibung abgegeben werden müssen, 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?

---

[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

**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!**

### 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.

Bitte führen Sie das Forschungstagebuch in digitaler Form; handschriftliche Abgaben werden nicht akzeptiert.

### Anhang: Qualität von Quellen

Ein wesentlicher Teil der Recherche 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/