Threat Modeling

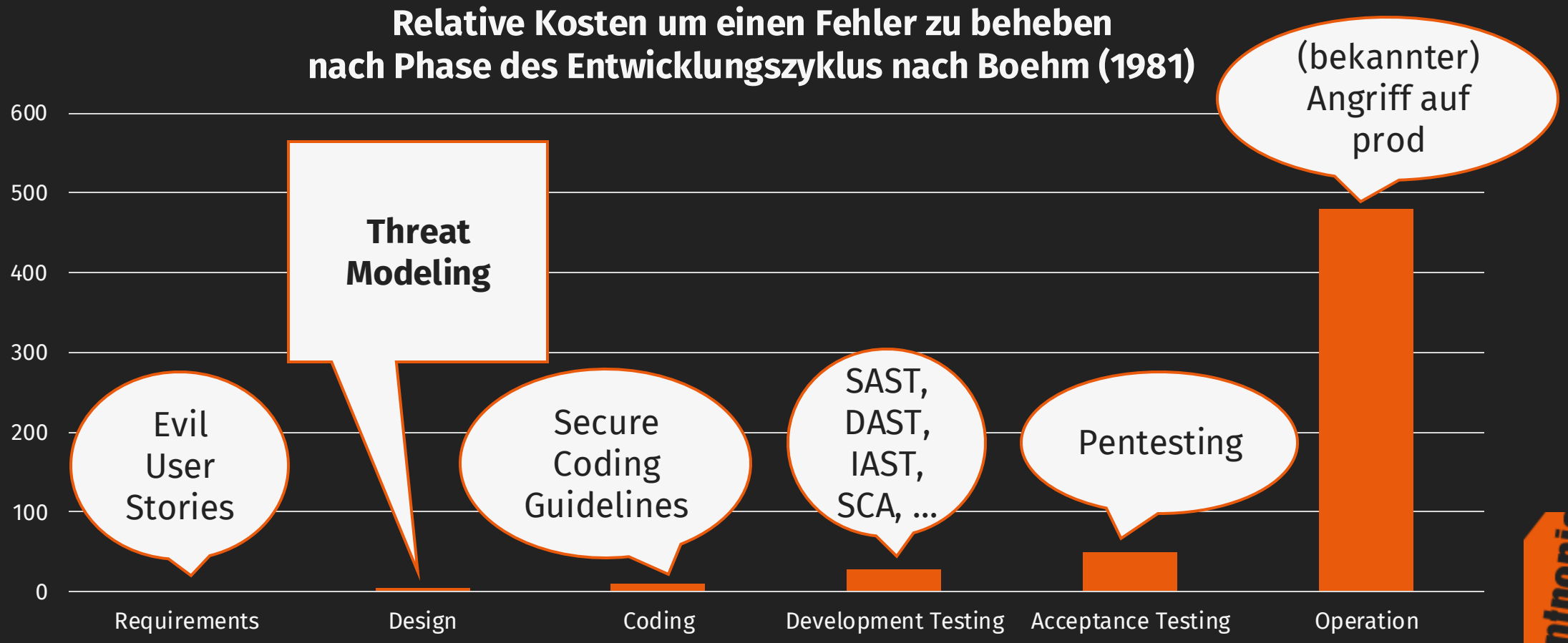
Jens / Entropia e.V.

Was lernen wir heute?

„Wenn wir Software entwickeln – woher wissen wir dann, worauf IT-Sicherheitstechnisch zu achten ist?“

— Ein schlauer Mensch, 2025

Warum brauchen wir proaktive Maßnahmen im Softwareentwicklungszyklus?



Quelle: „Error Cost Escalation Through the Project Life Cycle", Source of Acquisition, NASA Johnson Space Center, https://ntrs.nasa.gov/api/citations/20100036670/downloads/20100036670.pdf, zuletzt abgerufen am 12.12.2025

Threat Modeling...

1. ... ist eine strukturierte Methode zum Identifizieren von Bedrohungen und daraus abgeleiteten Sicherheitsanforderungen im Kontext bestimmter Angriffsszenarien.
2. ... wird initial während der „Design Time“ der Architektur der Anwendung durchgeführt.
3. ... ermöglicht eine Priorisierung der sicherheitsbezogenen Anforderungen und ein nachvollziehbares Risikomanagement.
4. ... kann auch bei agilem Vorgehen genutzt werden.

STRIDE

	Bedrohung	Gewollte Eigenschaft	Beispiele
S	**S**poofing (*Identitätsverschleierung*)	Authentizität	Als Admin anmelden, obwohl man nicht Admin ist; IP-Spoofing
T	**T**ampering (*Manipulation*)	Integrität	Im Online-Shop den Artikelpreis abändern, bevor man diesen in den Warenkorb legt
R	**R**epudiaton (*Verleugnung*)	Unabstreitbarkeit	Fünf Nutzer nutzen alle den `root`–Nutzer zum Anmelden auf einem Server
I	**I**nformation Disclosure (*Verletzung der Privatsphäre / Datenpanne*)	Vertraulichkeit	Abhören einer HTTP-Verbindung, die Kreditkartendaten enthält
D	**D**enial of Service (*Verweigerung des Dienstes*)	Verfügbarkeit	DDoS; Zip-Bombe; Kappen der Stromzufuhr
E	**E**levation of Privilege (*Rechteausweitung*)	Autorisierung	08/15-Nutzer kann `admin`-Nutzer löschen

Abwandlung: STRIDE-LM (Lateral Movement)

Vorgehensweise

- Shostack: Four Question Framework for Threat Modeling
  1. What are we working on *(right now)*?
  2. What can go wrong?
  3. What are we going to do about it?
  4. Did we do a good *(enough)* job?

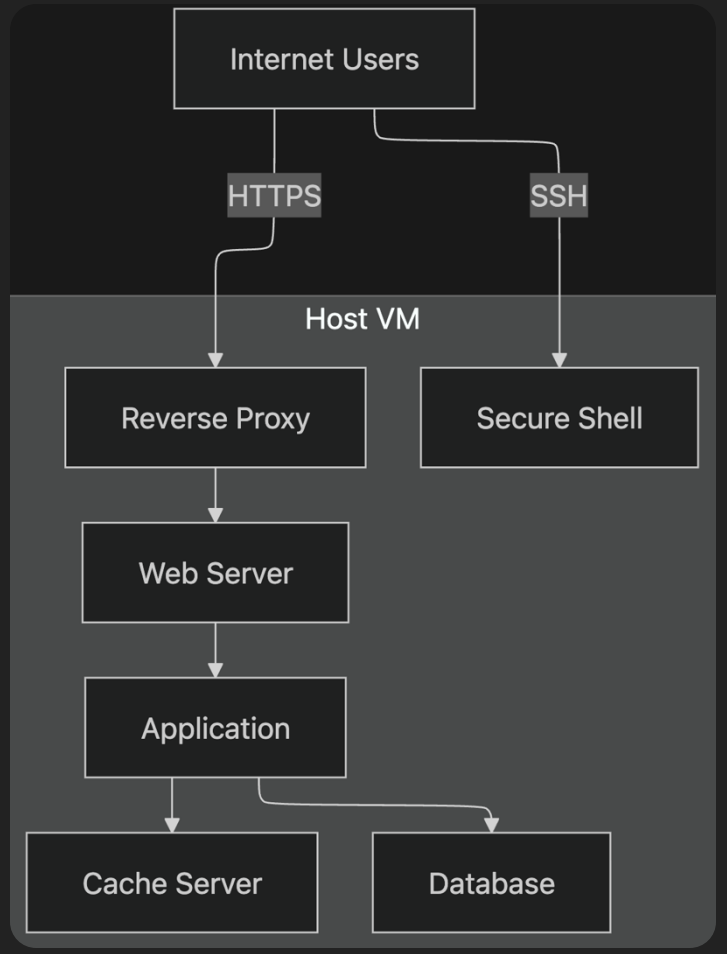
Quelle: „Understanding The Four-Question Framework for Threat Modeling", Shostack + Associates White Paper #5, November 2024, https://shostack.org/files/papers/The_Four_Question_Framework.pdf, zuletzt abgerufen am 13.12.2025

Setting: Bohnenkopf

- Bohnenkopf war mal Softwareentwickler, hat sich jetzt selbständig gemacht
- Kleine Kaffeerösterei möchte in der Online-Welt Fuß fassen
- Anforderungen: Kaffee-Blog, Forum für die Community, Live-Webcam von der Rösterei
- Wachsende Komplexität: User-Accounts, E-Commerce (Bestellungen), externe APIs (Barista).
- Problem: „Bohnenkopf“ ist zwar Security-interessiert, aber übermüdet (Caffeine-Crash) -> Bugs schleichen sich ein.
- Technologieauswahl: Linux VM (AlmaLinux) mit SSH-Server, Reverse Proxy (nginx), Web-Anwendung (WordPress), Datenbank (MariaDB), Cache (Valkey)

What are we working on (*right now*)?

- „Was sind meine Assets?“
- Datenflussdiagramm
- Zustandsübergangsdiagramm
- Bestandteile
  - Assets
  - Komponenten & Akteure
  - Trust Boundaries



What can go wrong?

- **Spoofing:** Angreifer erlangen durch Brute-Force oder Phishing Zugriff auf WordPress-Admin-Konten oder die Host-VM via SSH.
- **Tampering:** SQL-Injection in der Datenbank oder Cross-Site-Scripting (XSS) im Frontend.
- **Repudiation:** Fehlende Audit-Logs bei Admin-Aktionen oder das Löschen von System-Logs durch Angreifer.
- **Information Disclosure:** Path Traversal ermöglicht das Auslesen sensibler Dateien wie der `wp-config.php`.
- **Denial of Service:** HTTP-Flood (DDoS) auf den Nginx oder CPU-Überlastung durch SSH-Brute-Force.
- **Elevation of Privilege:** RCE-Schwachstellen in Plugins ermöglichen eine Shell im WordPress-Container.

What are we going to do about it?

- **S**poofing/**E**levation of Privilege: Passwörter, Patchmanagement, 2FA für Wordpress, Rate-Limiting am nginx & fail2ban
- **T**ampering with Data/**I**nformation Disclosure: Plugin-Minimalismus, Standard-Firewall, CSP, Containerisierung zur Dateisystem-Isolierung, HTTPS/HSTS mit Redirect
- **R**epudiation: Standard-Logging, Audit-Log-Plugin
- **D**enial of Service: Ausreichende Provisionierung, Caching für statische Inhalte & automatische Firewall-Anpassung durch Monitoring, bspw. fail2ban oder WAF

Did we do a good *(enough)* job?

- Besser wäre, eine Schutzbedarfsanalyse vorher durchzuführen um zu wissen, welchen Bedarf die Anwendung für uns hat

Toolunterstützung durch OWASP Threat Dragon

https://www.threatdragon.com/

Euer Raum für Fragen / Meinungen / Ahnung / Feedback