Selbstverteidigung für deine Applikation

Benjamin Brunzel
Rüdiger Heins

Online-Schwarzmarkt: Geklaute Kreditkarten und DDoS-Attacken für 'n Appel und 'n Ei

26.05.2016 11:08 Uhr – Dennis Schirrmacher vorlesen

(Bild: SecureWorks)

In Untergrund-Marktplätzen gehen Verkäufer neuerdings mit 24/7-Service auf Kundenfang. Oft wird versprochen, dass nur eine erfüllte Dienstleistung bezahlt werden muss, berichten Sicherheitsforscher.

Kryptologen vom Ciso Intel Team waren für SecureWorks in russischen Online-Schwarzmärkten unterwegs und zeigen neben aktuellen Preisen für kriminelle Leistungen auch neue Trends auf. Ihr Report Underground Hacker Markets erscheint jährlich und wurde in diesem Jahr zum dritten Mal veröffentlicht.

Von Kreditkarten bis zum Trojaner

Um die durchschnittlichen Preise für Diebesgut und illegale Dienstleistungen zu ermitteln, haben die Sicherheitsforscher eigenen Angaben zufolge verschiedene

Dienste

Security Consulter Emailcheck
Netzwerkcheck Browsercheck
Anti-Virus Krypto-Kampagne

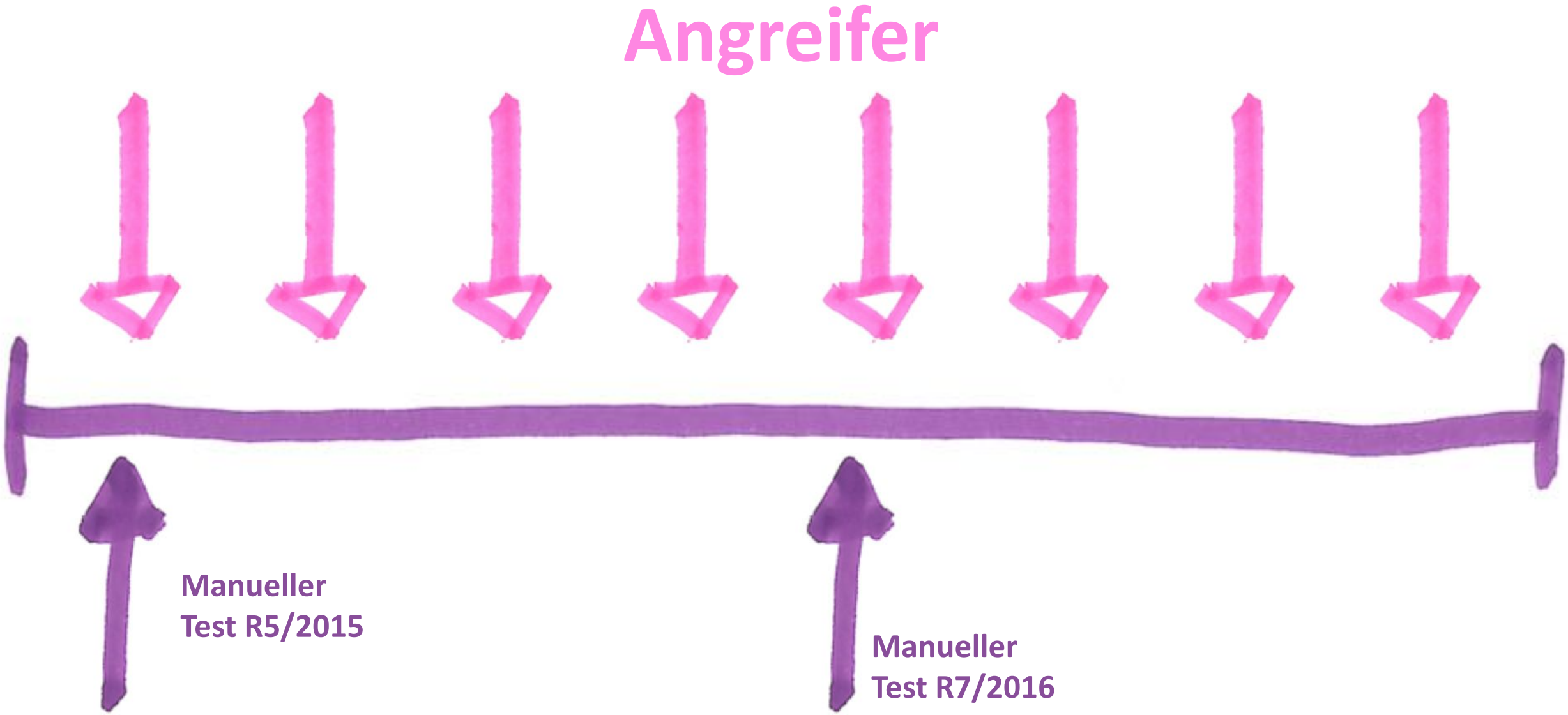
Artikel

PrivateBin: Pastebin-Alternative für Vertrauliches

PrivateBin verschlüsselt Inhalte, ist über das Tor-Netzwerk erreichbar und bietet einen Selbstzerstörungsmodus. Wer möchte, kann das Tool auch selbst auf seinem Server hosten.

Hardware-Fuzzing: Hintertüren und Fehler in CPUs aufspüren

Ein Prozessor-Fuzzer analysiert Hardware, der man normalerweise blind vertrauen muss. In ersten Testläufen


Angreifer
Manueller
Test R5/2015
Manueller
Test R7/2016
Verteidiger

```
buildscript {
    repositories {
        mavenCentral()
    }
    dependencies {
        classpath("org.springframework.boot:spring-boot-
gradle-plugin:1.5.15.RELEASE")
        classpath("org.owasp:dependency-check-gradle:3.3.1")
    }
}

apply plugin: 'org.owasp.dependencycheck‘
```

Was sollte ich ab morgen tun?

Bugs & Vulnerabilities

Leak Period: since previous version
started vor 4 Monaten

4 C	0 A	0	0
Bugs	Vulnerabilities	New Bugs	New Vulnerabilities

Code Smells

2d A	38	0	0
Debt	Code Smells	New Debt	New Code Smells

started vor 4 Monaten

Coverage

81.7%	313	—
Coverage	Unit Tests	Coverage on New Code

Duplications

6.2%	19	0.0%
Duplications	Duplicated Blocks	Duplications on 1 New Lines

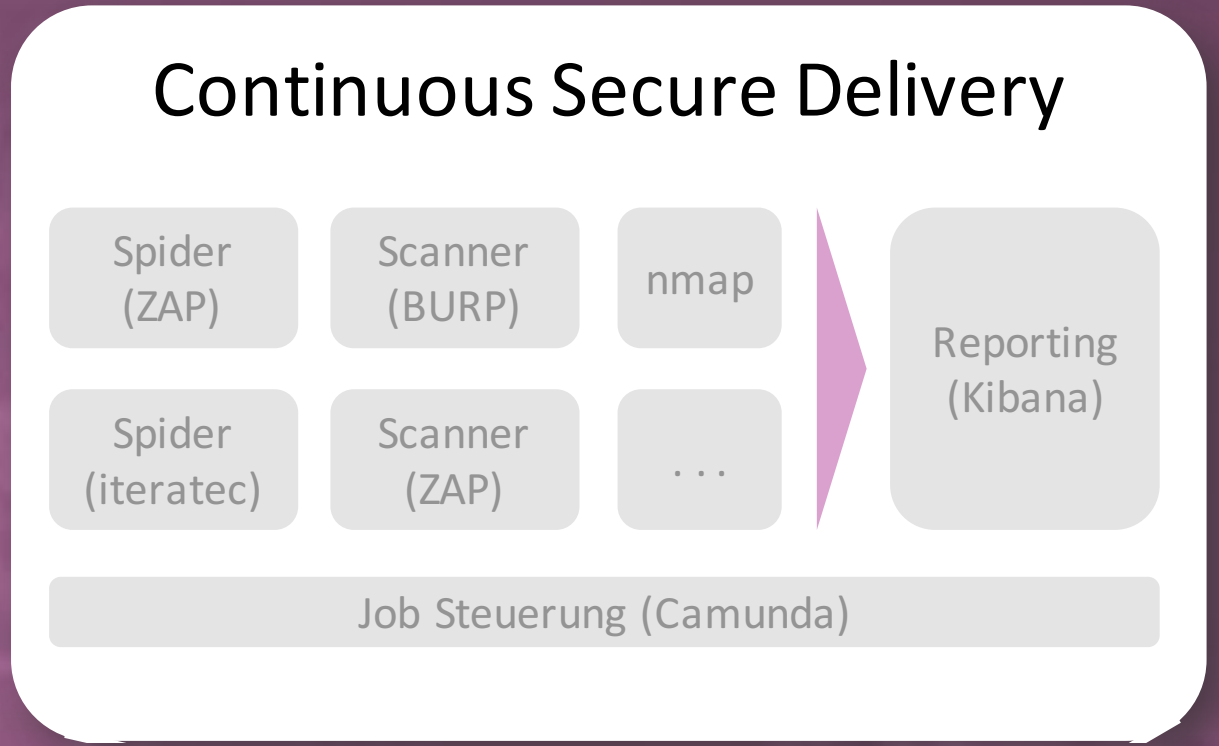
out-of-the-box

Cloud Ready

Plug ’n Play

µServices

hochskalierbar



Build

Int. Tests

Last Tests

Security Tests

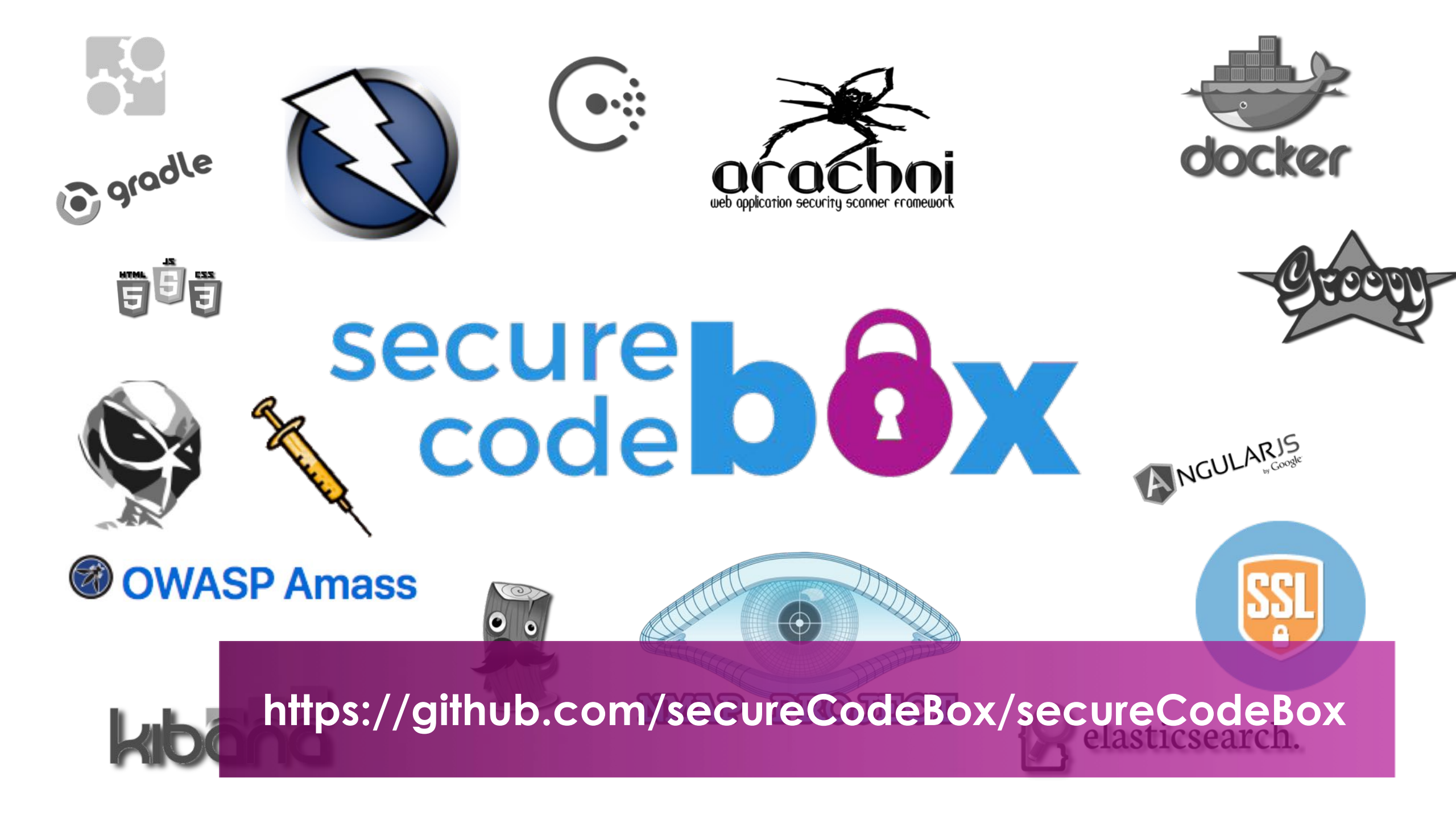
Release

Continuous Delivery

Werkzeuge der Angreifer nutzen

Low hanging fruits finden

... bevor es jemand anderes tut!


gradle
arachni
web application security scanner framework
docker
Groovy
secure
codebox
AngularJS
by Google
OWASP Amass
SSL
kibana
elasticsearch.
https://github.com/secureCodeBox/secureCodeBox

Perception!


Grafana


kibana


influxdb


elasticsearch


logstash

Demo Time ;)

Metriken

Womit starte ich?

- Login
  - Anzahl der erfolgreichen Logins
  - Anzahl der fehlgeschlagenen Logins
    - Differenz zwischen den Beiden.
  - Anzahl der Logouts (ggf. Fehlschläge)
  - Anzahl der Logins pro User-Konto
    - Top 10 Accounts (Datenschutz beachten)
- Sessions
  - Anzahl der aktiven Sessions / bekannte Token
  - Anzahl der Requests mit abgelaufener Session / Token
  - Anzahl der Requests mit ungültiger Session / Token
  - Anzahl der Refreshes
  - Durchschnittliche Sessionlänge
    - Top 10 Accounts (Datenschutz beachten)

Metriken

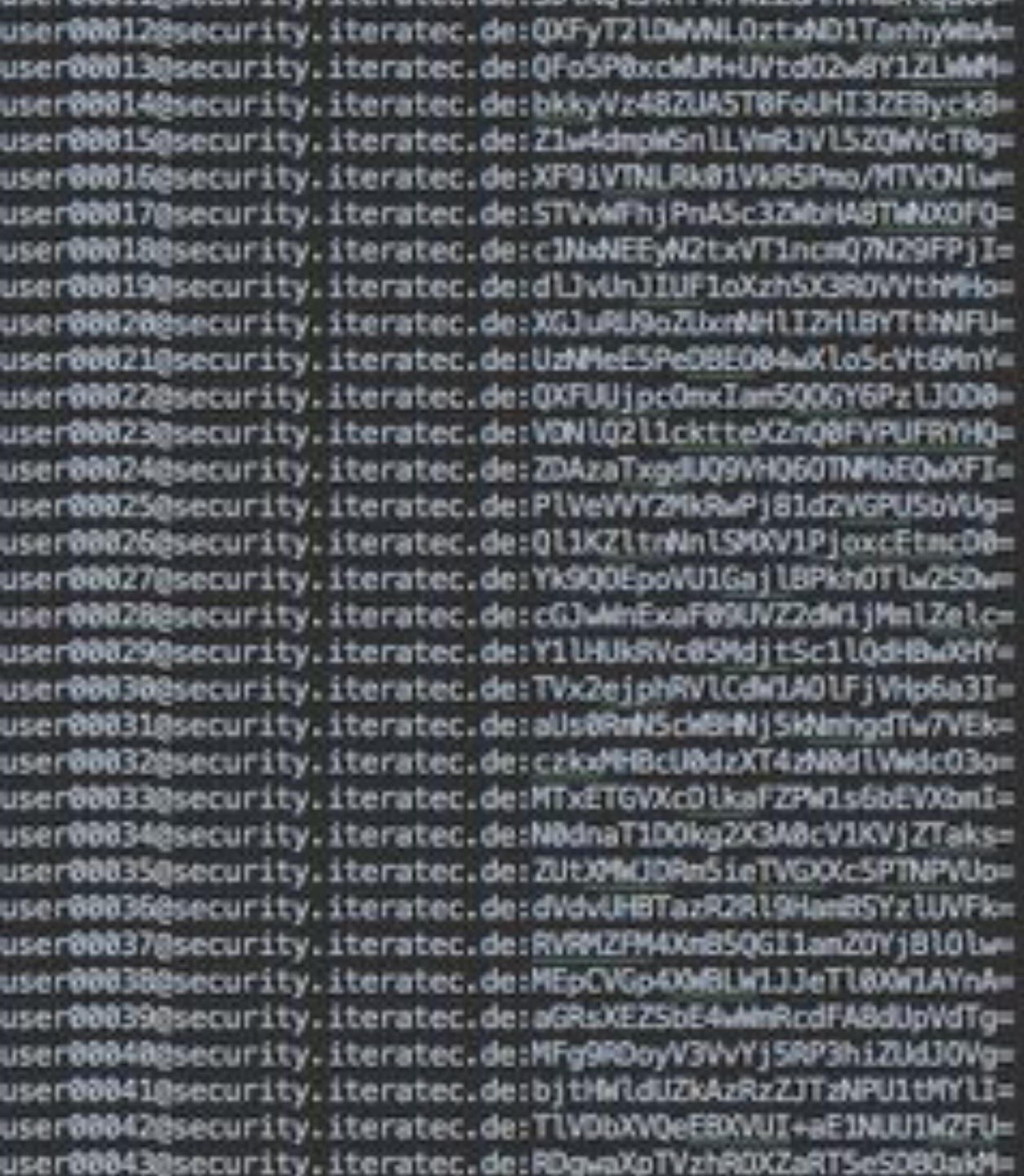
Womit starte ich?

- Allgemein / Fachlich
  - Aufrufrate der einzelnen Unterseite / Funktion
  - Fachliche Metriken:
    - Anzahl der Buchungen / Bestellungen
    - Anmeldung Newsletter
  - Anzahl Timeouts
  - Anzahl der Requests HTTP-1 vs HTTP-2
  - Validation Fehler

Interessante Request-Details

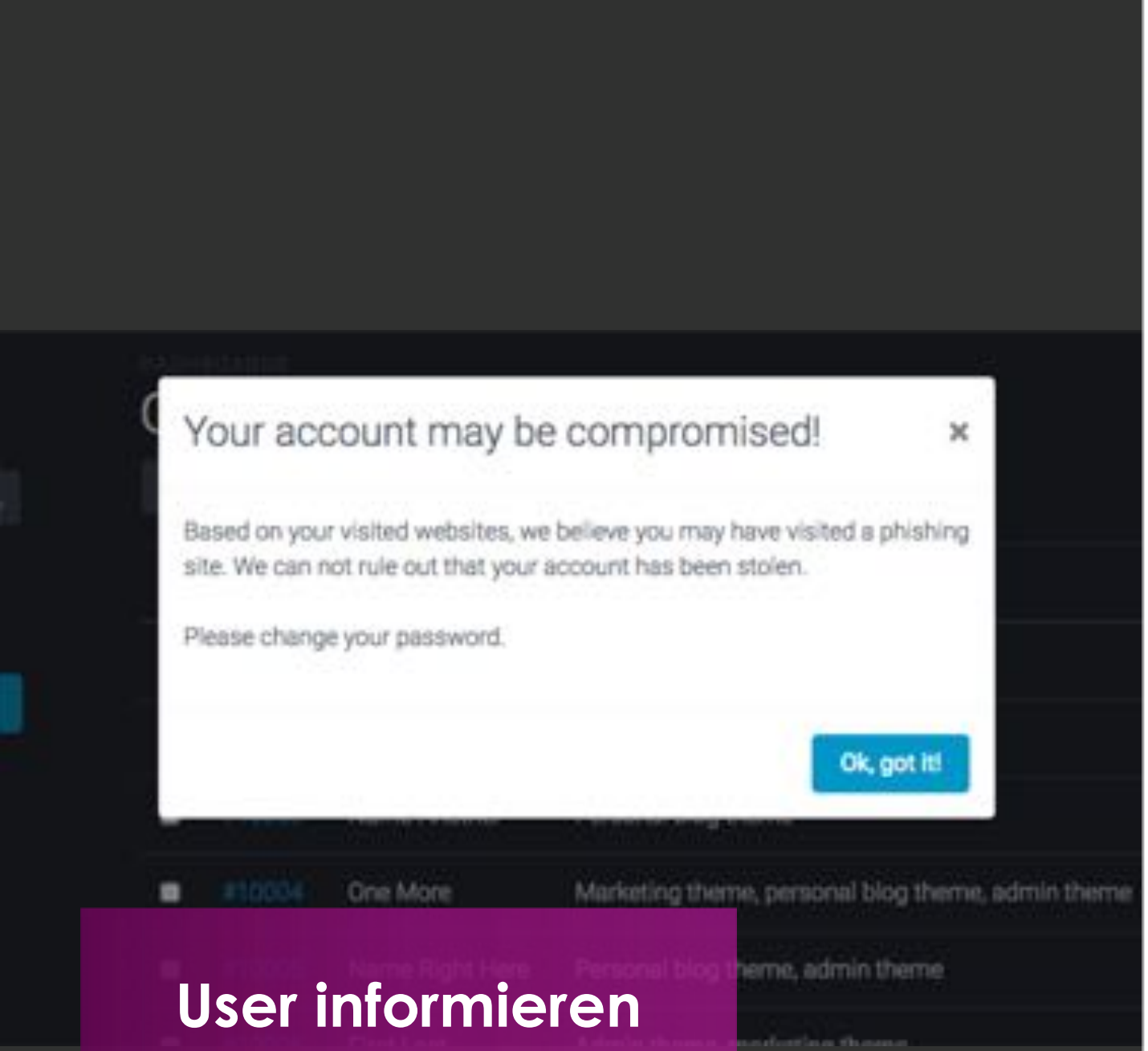
Metadaten

- Aufgerufene URL / Funktion
- Referer
- Accept-Header
- Accept-Encoding-Header
- Accept-Language-Header
- User-Agent-Header
- IP-Adresse-Header
- Beliebige Custom X-Header



Angriffe abwehren


Java-Script-Challenges

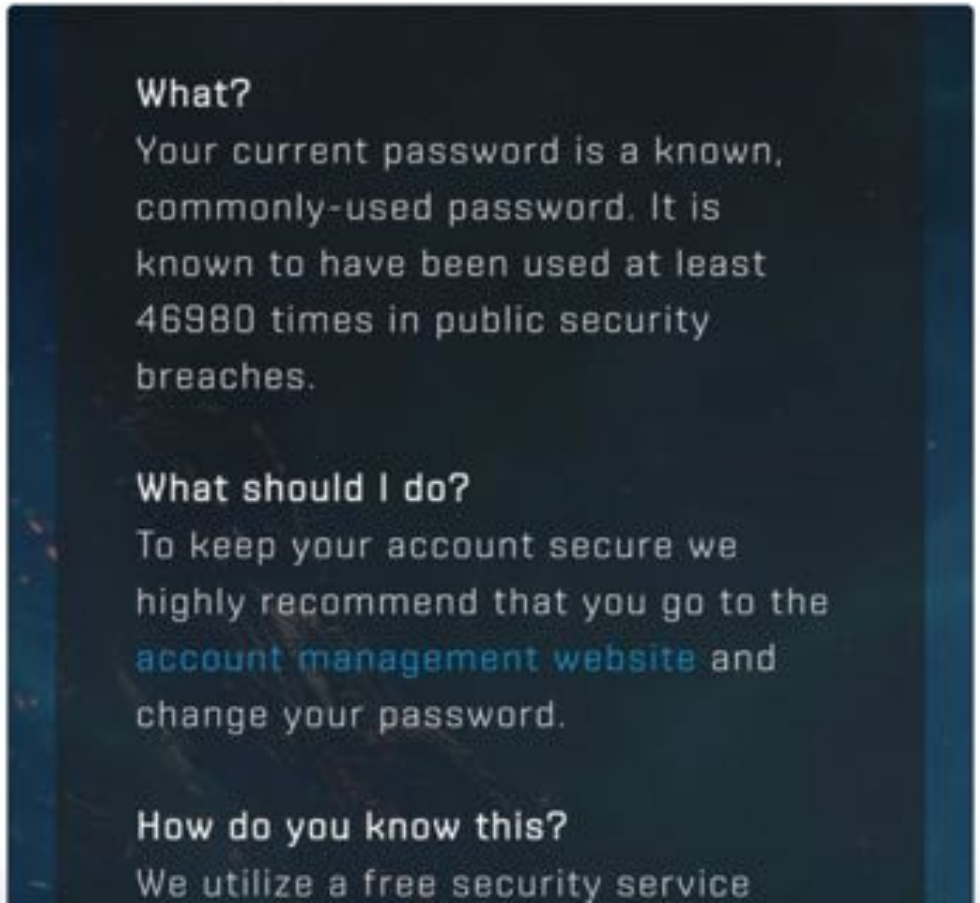


User informieren

Stefán Jökull Sigurðarson - CCP G...
@stebets

Folgen

WIP: Helping our @EveOnline players to be aware if their passwords are on a list of known compromised passwords. Thanks @haveibeenpwned ! CC: @troyhunt #tweetfleet #security #workinprogress



Honeypot

Summary

Was mache ich ab Morgen?

- Dependency-Scanner in die Build einbauen

- Eintrittsaktionen loggen und monitoren
- Fachliche Bedrohungen mit Bedrohungsanalysen identifizieren
- Gegenmaßnahmen ermitteln und umsetzen

- Checkout GitHub: https://github.com/iteratec/security-karate

- https://github.com/iteratec/secureCodeBox

Kontakt

Benjamin Brunzel | Rüdiger Heins
@asciijungle @therockinbear

Benjamin.Brunzel@iteratec.de | *Rüdiger.Heins@iteratec.de*
Am Sandtorkai 75
20457 Hamburg

Weiterführende Links & Quellen

- https://www.owasp.org/index.php/Logging_Cheat_Sheet
- https://www.owasp.org/index.php/OWASP_Security_Logging_Project
- https://www.owasp.org/images/b/b2/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf
- https://www.digitalocean.com/community/tutorials/an-introduction-to-metrics-monitoring-and-alerting
- https://www.owasp.org/index.php/OWASP_Proactive_Controls#8:_Implement_Logging_and_Intrusion_Detection
- Photos by sebastiaan stam, Tobias Mrzyk, Eric Ward, Patrick Fore, Markus Spiske on Unsplash