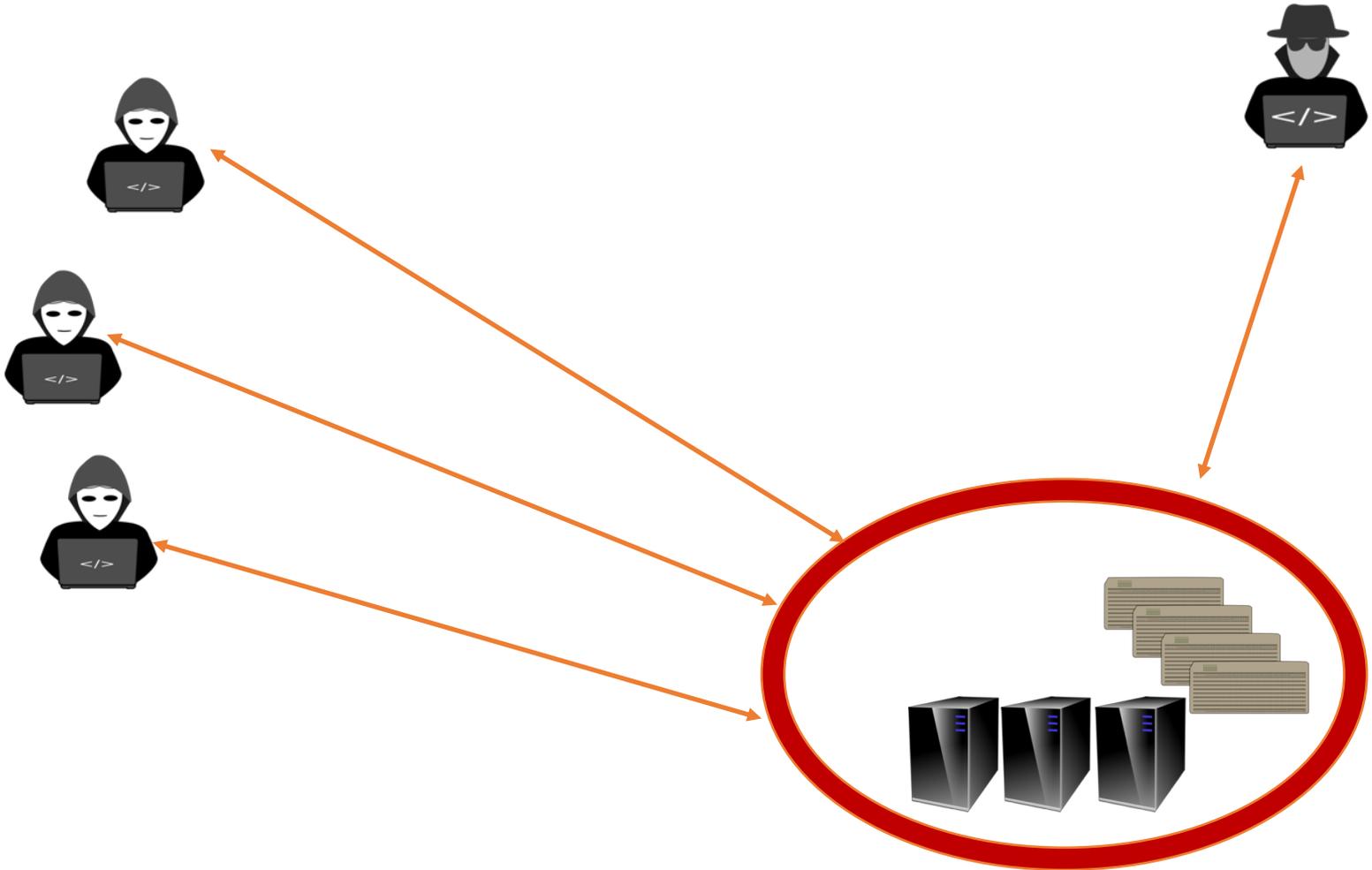


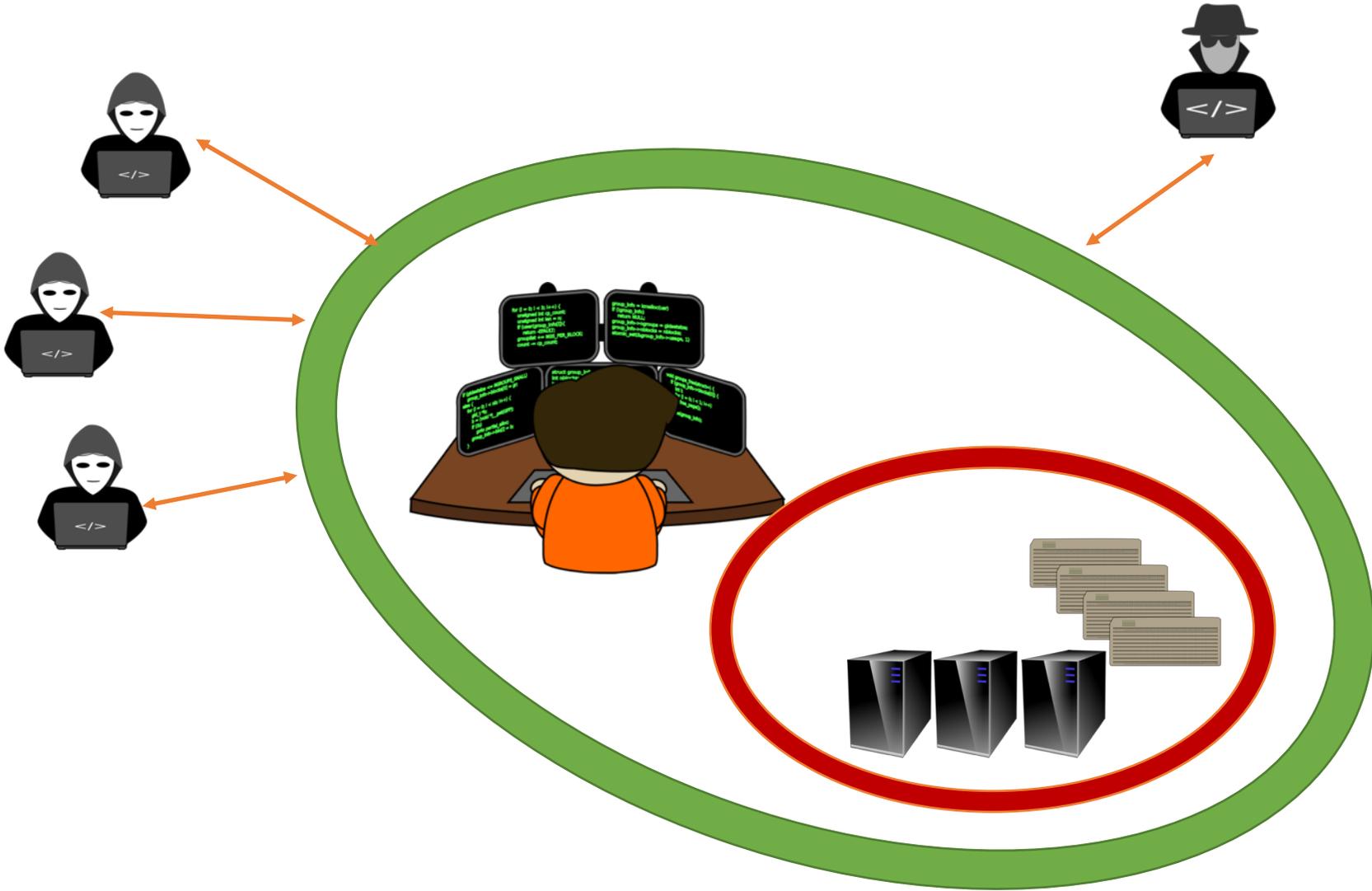
Projektgruppe Entwicklung automatischer Tools zur Lösung von CTFs

Simon Dierl, Malte Mues, Prof. Dr. Falk Howar

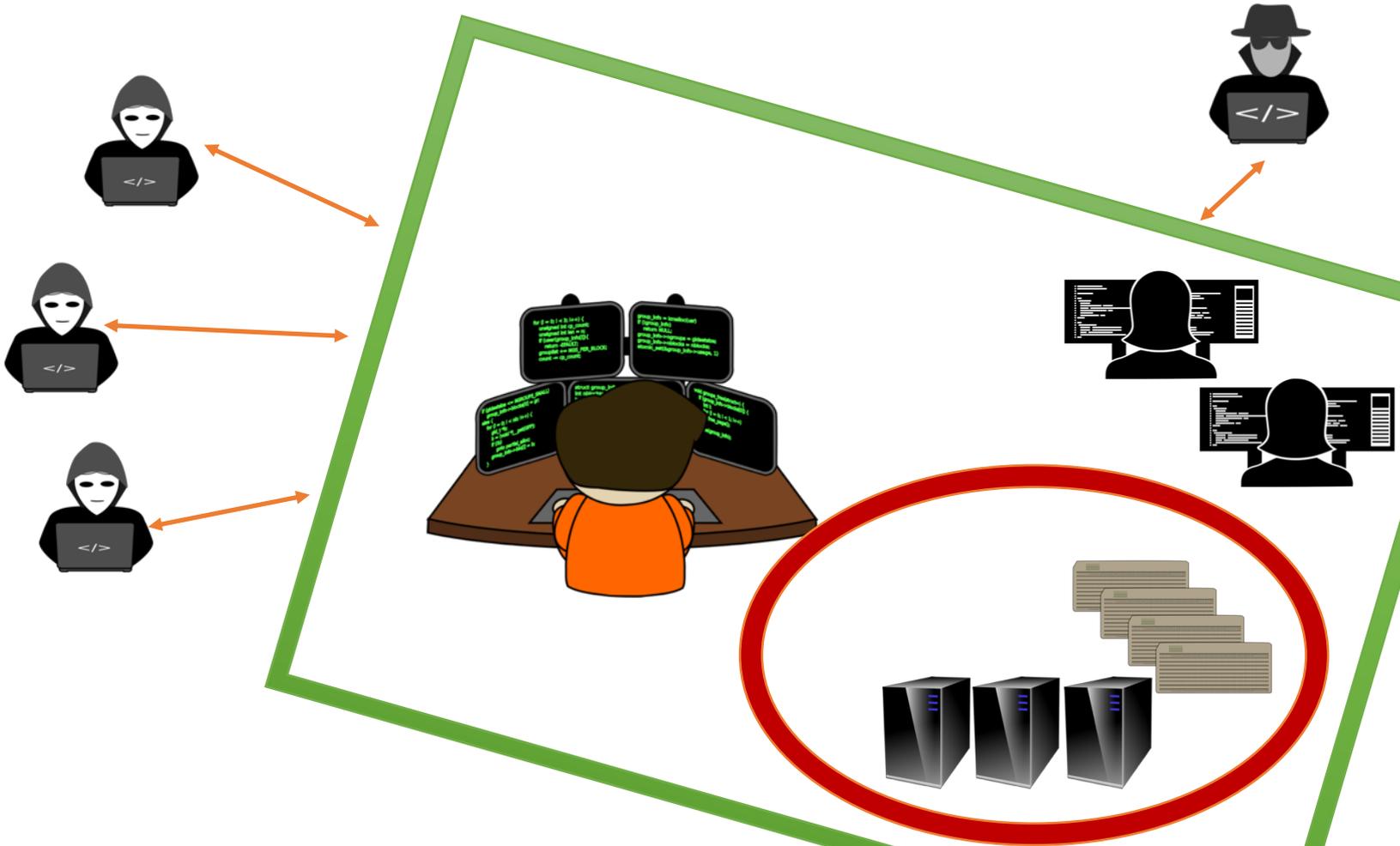
Problemstellung



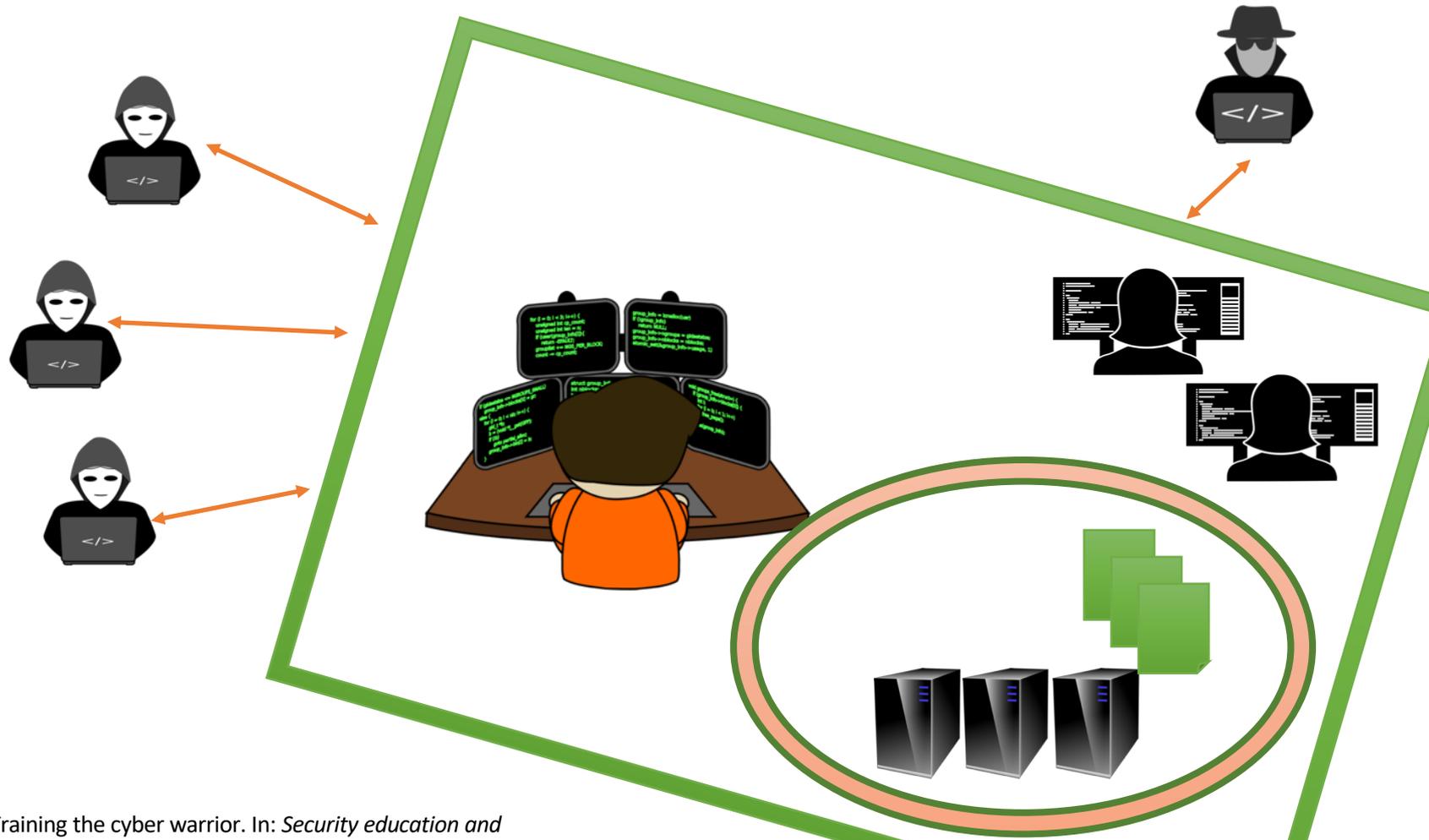
Problemstellung



Problemstellung



Problemstellung



FULP, J. D. Training the cyber warrior. In: *Security education and critical infrastructures*. Springer, Boston, MA, 2003. S. 261-273.

Angriffe auf den Bundestag

Cyberangriff
+++Generalbundesanwalt schaltet sich ein+++
 Unbekannte haben persönliche Daten und Dokumente von Künstlern, Journalisten und Politikern ins Netz gestellt. Die Generalbundesanwalt hat sich inzwischen eingeschaltet. Die Entwicklungen im Liveblog | mehr

Hackerangriff auf Hunderte deutsche Politiker

Wer steckt hinter der Attacke?
 Die Liste der vom Hackerangriff betroffenen Personen ist lang. Während die AfD verschont blieb, wurden Politiker, Künstler und Journalisten geschädigt, die oft von rechts attackiert werden. Von Patrick Gensing | mehr

#faktenfinder

Hintergrund
 Internetkriminalität
Experten nennen es Doxing
 Wie nennt man es, wenn private Daten unerlaubt ins Netz landen? Hack? Oder Cyberattacke? Experten sprechen im vorliegenden Fall von Doxing. Das Wort

Nach Cyberattacke Ermittlungen und Empörung
 Die Bundesregierung wertet die Hackerattacke auf Politiker, Künstler und Journalisten als "schwerwiegenden Angriff". Sicherheitsbehörden prüfen weitere Schritte

Spurensuche
Cyberangriff - was bisher bekannt ist
 Die massenhafte Veröffentlichung sensibler Daten im Internet wirft viele Fragen auf: Wer ist steckt hinter dem Cyberangriff? Wer ist betroffen? Und wie sieht es jetzt weiter?

GEHEIMDIENSTLICHE AGENTENTÄTIGKEIT
Generalbundesanwalt sucht die Bundestagshacker

Seit dem Hackerangriff auf den Deutschen Bundestag sind mittlerweile rund acht Monate vergangen - jetzt hat der Generalbundesanwalt Ermittlungen aufgenommen, um die Täter zu finden. Verdächtig wird ein ausländischer Geheimdienst.

21. Januar 2016, 10:26 Uhr, Hauke Gierow

HACKERANGRIFF
Bundestag schaltet sein Computersystem ab

Das Computersystem angelegter Hackera werden jetzt über...

Spionageverdacht
Hacker drangen in deutsches Regierungnetz ein
 Ausländische Hacker haben das bislang als sicher geltende Datennetzwerk des Bundes und der Sicherheitsbehörden infiltriert. Verdächtig wird angeblich jene Gruppe, die 2015 den Bundestag gehackt hatte.

Anlass dafür war ein groß... Die Systeme...
 Pakalski/dpa

Auswärtiges Amt in Berlin

Mittwoch, 28.02.2016 17:18 Uhr
 Drucken Nutzungsrechte Feedback

<https://www.golem.de/news/hackerangriff-bundestag-schaltet-sein-computersystem-ab-1508-115879.html>
<https://www.golem.de/news/geheimdienstliche-agententaetigkeit-generalbundesanwalt-sucht-die-bundestagshacker-1601-118658.html>
<https://www.tagesschau.de/newsticker/liveblog-hack-politiker-101.html#Generalbundesanwalt-prueft-Angriff>
<http://www.spiegel.de/netzwelt/netzpolitik/bundesregierung-hacker-sind-angeblich-in-regierungsnetz-eingedrungen-a-1195890.html>

Generalbundesanwalt prüft Angriff
 12:42 Uhr

Der Generalbundesanwalt hat sich in die Prüfung des Angriffs eingeschaltet. Dazu sei in der Behörde in Karlsruhe ein sogenannter Beobachtungsvorgang angelegt worden, sagte eine Sprecherin des Bundesjustizministeriums. Damit untersucht der Generalbundesanwalt die Bedeutung des Falls und die kriminelle Relevanz und prüft, ob er weiter tätig wird.

Die Bundesanwaltschaft wäre insbesondere für Ermittlungen bei "geheimdienstlicher Agententätigkeit" zuständig, also wenn sich herausstellen sollte, dass eine ausländische Macht hinter den Vorgängen stecken könnte.

Passwörter

München 0°

Süddeutsche Zeitung

SZ.de Zeitung Magazin

Politik Wirtschaft Panorama Sport München Bayern Kultur Gesellschaft Wissen Digital

Hacker-Angriff

Die wichtigsten Antworten zu den geleakten Dateien



Unbekannte haben sensible Informationen von Politikern, Prominenten und Journalisten veröffentlicht. Wer steckt dahinter? Was enthält das Leak? Und wie sind die Angreifer an die Daten gelangt?

Von Jana Anzlinger, Constanze von Bullion, Simon Hurtz und Hakan Tanriverdi

Ein tyrannischer Akt

Wer auch immer die Daten von Prominenten und Politikern an die Öffentlichkeit gezeit hat, er nutzt die Möglichkeiten des Internets zum Schlechtesten. Der Datenklau führt vor, wie verletzlich jeder ist, der sich im Netz bewegt.

So gehen sichere Passwörter

Hacker haben persönliche Daten von vielen Politikern und Prominenten abgegriffen. Eine 100-prozentige Sicherheit gibt es nicht, aber diese sieben Empfehlungen helfen Ihnen, Ihre Konten zu sichern und gute Passwörter zu vergeben.



schwer verletzt: Kripo ermittelt

vor 7 Min. Wetter -

UNCOMMON (NON-GIBBERISH) BASE WORD

ORDER UNKNOWN

Tr0ub4dor &3

CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS EXACTLY ONE OF A FEW COMMON SERVICES)

~ 28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(PLAUSIBLE ATTACK ON A WEAK SERVICE WITH SERVICE, YES, CROWDING A STRONG HEAVY IS PROTECT, BUT IT'S NOT WHAT THE ANGRY USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: HARD

correct horse battery staple

FOUR RANDOM COMMON WORDS

~ 44 BITS OF ENTROPY

$2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: HARD

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

<https://xkcd.com/936/>

Beispiele

- goto fail (2014): entfernte Umgehung von Authentifizierung
- Heartbleed (2014): entfernter Zugriff auf private Schlüssel und Benutzerdaten
- ShellShock (2014): entfernte Codeausführung
- Dirty COW (2016): lokale Rechteerweiterung
- iamroot (2017): lokale Rechteerweiterung
- ROBOT (2018): entfernte Rückberechnung privater Schlüssel

Lösung: Bug Bounties

EU to fund bug bounty program for top open-source software

By Anthony Spadafora 4 days ago Software

14 popular open-source projects will be funded in the third edition of FOSSA



The European Union will help cover the expenses of bug bounty programs for 14 open-source projects according to an announcement made by EU Member of Parliament Julia Reda.

<https://www.techradar.com/news/eu-to-fund-bug-bounty-program-for-top-open-source-software>

Buffer overread

```
void CWE126_Buffer_Overread__char_alloca_loop_01_bad()
{
    char * data;
    char * dataBuffer = (char *)ALLOCA(50*sizeof(char));
    ...
    data = dataBuffer;
    {
        size_t i, destLen;
        char dest[100];
        ...
        destLen = strlen(dest);
        for (i = 0; i < destLen; i++)
        {
            dest[i] = data[i];
        }
        dest[100-1] = '\0';
        printLine(dest);
    }
}
```

BOLAND, Tim; BLACK, Paul E. Juliet 1. 1 C/C++ and Java Test Suite. *Computer*, 2012, 45. Jg., Nr. 10, S. 88-90.

Buffer overread

```
void CWE126_Buffer_Overread__char_alloca_loop_01_bad()
{
    char * data;
    char * dataBuffer = (char *)ALLOCA(50*sizeof(char));
    ...
    data = dataBuffer;
    {
        size_t i, destLen;
        char dest[100];
        ...
        destLen = strlen(dest);
        for (i = 0; i < destLen; i++)
        {
            dest[i] = data[i];
        }
        dest[100-1] = '\0';
        printLine(dest);
    }
}
```

Dynamisches Char-Array 50

Stack Char-Array 100

Integer [0, 100)

Read: $i < \text{data.size}$

Write: $i < \text{dest.size}$

Challenges

- Dateisysteminteraktion
- Netzwerke
- Framework
- Fehlerbehandlung
- Portierbarkeit
- Methodenaufrufe

Mögliche Tools

- JDart, SPF, JBMC
- CBMC, CPA-Checker, SMACK
- SMT-Solver (z.B.: Z3, SMTInterpol, Princess, CVC4)
- Learnlib, RA-Lib
- Theorem Prover (z.B.: Coq, Isabelle, HOL light, PVS)
- Etablierte Tools: Metasploit, nmap, Valgrind, Wireshark, Hydra, PMD, nslookup ...

Demo



https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

Idee zum Vorgehen

- VM hacken und Capture the Flag Challenges (CTFs) lösen
- Sicherheitsprobleme verstehen (CWE und CVE)
- Aktuelle Tools verstehen und ausprobieren
- Eigenes Problem suchen und Tools automatisieren
- Design von Benchmark CTFs



Zeit

Was könnt ihr lernen?

- Sicherheitslücken verstehen
- Dynamische und Statische Code-Analyse
- Qualitätssicherung
- Erfahrungen mit formalen Methoden
- Deduktive KI-Ansätze mittels Theorem Proving

Was bringt ihr mit?

- Pflicht:
 - Erfahrung mit einer Hochsprache
 - Erfahrung mit einer Skriptsprache
- Optional:
 - Performance Benchmarks
 - Infrastruktur (OS, Netzwerke, Virtualisierung)
 - Kenntnisse über Sicherheitslücken
 - Formale Methoden

Ziele

- Minimal:
 - 2 CTF-VMs mit mindestens 4 didaktischen Beispielen, welche dokumentiert sind und durch Tools automatisch erfolgreich attackiert werden.
- Optional:
 - <https://www.hackerone.com/internet-bug-bounty>
(Nach der PG)
 - <https://ctftime.org/event/list/>
 - ...

Anregungen

- <https://www.vulnhub.com>
- <https://www.hacker101.com>
- <https://samate.nist.gov/SARD/testsuite.php> (nach US-Government shutdown)

- <https://github.com/psycopaths/jdart>
- <https://github.com/diffblue/cbmc>
- <https://learnlib.de>
- <https://rise4fun.com>
- <https://www.kali.org/kali-linux-documentation/>
- <https://blackarch.org>

Projektgruppe Entwicklung automatischer Tools zur Lösung von CTFs

Fragen?