Cyber Security Workshop

Praxisorientiertes Fachwissen und Fertigkeiten im Bereich IT-Sicherheit

Über uns

- Patrick Eisoldt
  - Studium: Hochschule Albstadt-Sigmaringen und Glyndwr University in Wales
  - Praktika/Thesen: Siemens, Marquardt
  - November 2010 bis August 2011: Mitarbeiter Digitale Forensik
  - Seit 2012: Mitarbeiter Open C³S
  - Schwerpunkte: Digitale Forensik, Windows-Forensik, Python (Forensik und Pen-Tests)

Über uns

- Tobias Scheible
  - Studium: Kommunikations- und Softwaretechnik, Fachrichtung Kommunikationstechnik, Hochschule Albstadt-Sigmaringen
  - Diplomarbeit: Erhebung von Anforderungen an asynchrone Web-Anwendungen
  - 2009 bis 2012: Web Development & Online-Marketing, Gute Aussicht Kommunikations GmbH
  - Seit 2012: Mitarbeiter IWW - Open C³S
  - Schwerpunkte: Internet Technologien, Frontend Development, Web Vulnerability Scans und Cloud Computing

Vorstellungsrunde

- Wie heißt ihr und wo kommt ihr her?
- Welches Fach studiert ihr und in welchem Semester seid ihr?
- Habt ihr bereits Erfahrungen im Bereich Cyber Security?
- Was ist eure Motivation für die Teilnahme am Workshop?

Workshop Agenda

- Cyber Security
- System Security
- Data Security
- E-Mail Security
- Internet Security
- Cyber Defense

- Hinweis: Präsentation, Beispiel-Dateien und Links bald auf der Website


Cyber Security

Workshop Agenda

- Cyber Security
  - » Security Grundlagen
  - » Sicherheitswerkzeuge
- System Security
- Data Security
- E-Mail Security
- Internet Security
- Cyber Defense

Security Grundlagen

- Gesetzliche Grundlagen
  - » Computersabotage, Kreditkartenbetrug, ...
  - » Hackerparagraph
- Schwachstellen
  - » Anzahl der Benutzer
  - » IT-Kenntnisse der Benutzer
  - » Vorhandene Software

Security Grundlagen

- Angreifer
  - » Hacker, Cracker, Kriminelle, Skriptkiddie, Spione und Saboteure
- Angriffsmethoden
  - » Man-in-the-Middle, Spoofing, Phishing, DOS, Seitenkanalattacke
- Angriffswerkzeug
  - » Viren, Würmer, Trojaner, Hoaxes, Spyware, Rootkit, Exploit, Botnetz
- Schutzziele
  - » Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit, Verbindlichkeit

Security Grundlagen

- Angriffsarten
  - » passive Angriffe
    - › Beispiel: WLAN Daten abfangen
  - » aktive Angriffe
    - › Beispiel: Brute-Force-Methode
  - » externe Angriffe
    - › Beispiel: Krimineller
  - » interne Angriffe
    - › Beispiel: Praktikanten

Security Grundlagen

- Metadaten
  - » Beispiele: Stanford Experiment
    - › „Eine Teilnehmerin telefonierte morgens lange mit ihrer Schwester. Zwei Tage danach rief sie mehrere Stellen für Schwangerschaftsberatung an und zwei Wochen danach noch einmal. Einen Monat später tätigte sie einen letzten Anruf bei einer der Stellen."
    - › „Ein anderer Proband kontaktierte im Zeitraum von drei Wochen einen Baumarkt, einen Schlosser sowie Firmen, die Hydrokulturgeräte vertreiben und einen Fachhändler für Drogenzubehör."
  - » Beispiele: Electronic Frontier Foundation
    - › „Sie weiß, dass Sie den Hilfsdienst der Golden Gate Bridge für Selbstmörder angerufen haben, aber das Thema des Anrufs bleibt geheim."
    - › „Sie weiß, dass Sie mit einem Dienst für HIV-Tests telefoniert haben und kurz danach mit Ihrem Arzt und Ihrer Krankenversicherung. Aber worüber gesprochen wurde, weiß sie nicht."

Sicherheitswerkzeuge

- Live-Systeme
  - » Betriebssystem ohne Installation
  - » Sichere Umgebung
  - » Werkzeugkasten: Lokales System bearbeiten
  - » Es gibt verschiedene Ansätze z. B. Heise Desinfec’t, Bankix, Surfix, Kali
- Virtuelle Maschine
  - » Hardware durch Software simuliert
  - » Einfachere Handhabung, aber möglicher Angriffsvektor

- Praxis: Live-USB-Stick

System Security

Workshop Agenda

- Cyber Security
- System Security
  - » Sicherheit von Passwörtern
  - » Passwortschutz
- Data Security
- E-Mail Security
- Internet Security
- Cyber Defense

Sicherheit von Passwörtern

- Wie sieht ein sicheres Passwort aus?
  - » Mindestens 10 Zeichen
  - » Neben Groß- und Kleinbuchstaben auch Umlaute und Sonderzeichen
  - » Keine Begriffe aus Wörterbüchern
- Angriffe auf Passwörter
  - » Wörterbuchangriff
  - » Bekannte Ersetzungsmethoden
  - » Brute force

- Beispiel: Wie schnell kann ein Passwort geknackt werden?

Sicherheit von Passwörtern

- Eselsbrücken
  - » 3 beliebige Wörter (Vorteil: Smartphone u. Tablet)
  - » Anfangsbuchstaben eines willkürlichen Satzes + Sonderzeichen
  - » Tipp: Dialekt verwenden
- Best Practice
  1. Nie das gleiche Passwort für mehrere Dienste verwenden
  2. Bei wichtigen Daten regelmäßig Passwörter ändern
  3. Schwachstellen „kennen“ und Risiko abschätzen

  - » Praxis: Firefox-Passwort Speicherung erzwingen & knacken

Passwortschutz

- PDF-Passwortschutz
  - » Die Stärke des Schutzes ist abhängig von der verwendeten Technik
  - » Die Länge des Passwortes ist häufig entscheidend

  - » Praxis: Windows Passwort umgehen
  - » Praxis: PDF Passwort knacken

Data Security

Workshop Agenda

- Cyber Security
- System Security
- Data Security
  - » Daten verschlüsseln
  - » gelöschte Daten wiederherstellen
- E-Mail Security
- Internet Security
- Cyber Defense

Daten verschlüsseln

- 7zip
  - » Schnelle unkomplizierte Verschlüsselung
- TrueCrypt
  - » Etwas aufwendiger
  - » Container
  - » Festplatte mit Bootloader
- Ein verschlüsselter Container kann jederzeit gelöscht werden!

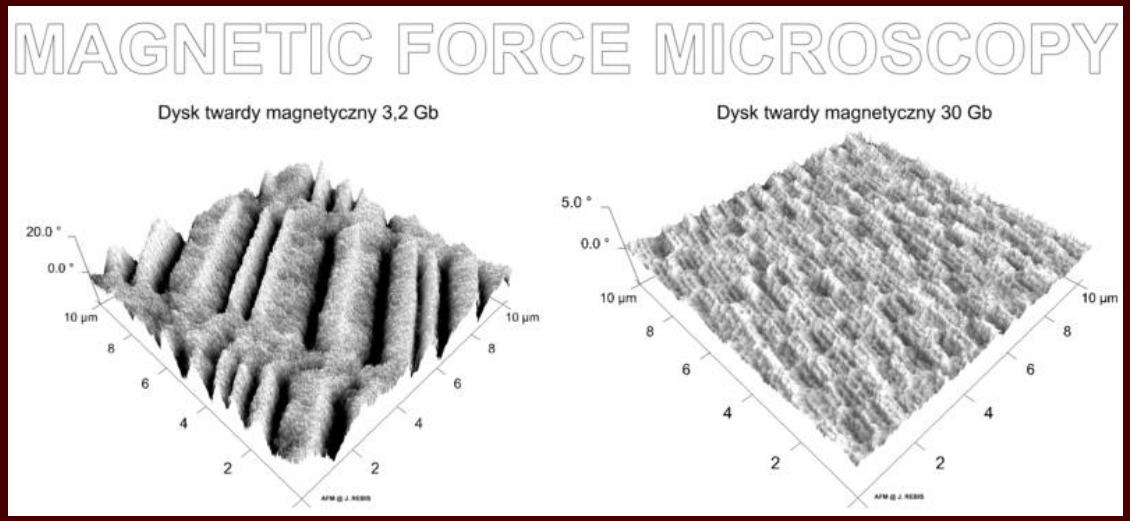
Gelöschte Daten wiederherstellen

- Wie arbeitet ein Dateisystem?
  - » Vergleich: Festplatte = Enzyklopädie (unsortiert)
  - » Zentrales Dateiverzeichnis = Inhaltsverzeichnis der Enzyklopädie
  - » Dateiverzeichnis enthält verschiedene Attribute (z. B. Verweis auf Speicherort)
  - » Eintrag gelöscht → Datei „unauffindbar“
  - » → Carving
- Worst Case Vorgehen

- Praxis: Daten mit Recuva wiederherstellen

Sicheres Löschen

- Sicheres Löschen wird nur durch Überschreiben erreicht
- Alle Sektoren einer Festplatte müssen überschrieben werden
- Restmagnetisierung: Wie oft muss eine Festplatte beschrieben werden?
  - » Datenüberschreibung = Datenzerstörung (NIST 2006)



Disk Wipe

- Sicheres Löschen unter Windows
- Benötigt keine Installation
- Windows-Partition kann nicht gelöscht werden

- Praxis: Daten mit Disk Wipe löschen

Live-System für das sichere Löschen

- „Verbaute“ Festplatte mit Linux löschen
- Funktioniert mit jedem Linux
- Ggf. mit `apt-get install <Paketname>` nachinstallieren
- Gezieltes Löschen und vollständiges Löschen der Festplatte möglich

Gezieltes Löschen

- Gezieltes Löschen einer Datei mit `shred`
  - `shred <Dateiname>`
- Die Datei wird „nur“ überschrieben (25x)
- Das anschließende Löschen ist optional
  - `shred -remove <Dateiname>`

Vollständiges Löschen

- In der Konsole die richtige Festplatte ermitteln
  - `sudo fdisk -l`
- Anschließend mit dd die Festplatte formatieren
  - `dd if=/dev/zero of=/dev/<Festplattenname>`
- `/dev/zero` ist eine virtuelle Gerätedatei, die das Nullzeichen liefert

E-Mail Security

Workshop Agenda

- Cyber Security
- System Security
- Data Security
- E-Mail Security
  - » E-Mails digital signieren
  - » E-Mail Kommunikation verschlüsseln
- Internet Security
- Cyber Defense

E-Mails digital signieren

- E-Mail Kommunikation
  - » Verbindung standardmäßig unverschlüsselt
  - » Keine Verifikation des Absenders
  - » E-Mails liegen offen auf den E-Mail-Servern
  - » Verschlüsselte Verbindungen nur zum eigenen E-Mail-Server

  - » Praxis: Spam, E-Mail Absender fälschen & TLS/SSL-Verbindung testen

E-Mails digital signieren

- S/MIME-Verfahren
  - » S/MIME (Secure / Multipurpose Internet Mail Extensions) ist ein Standard für die Verschlüsselung und Signatur von E-Mails
  - » Der Standard wird von vielen E-Mail Anwendungen unterstützt
  - » Public-/Private-Key-Verfahren auf Basis von Zertifikaten
  - » Nur signierte E-Mails können von jedem E-Mail Programm angezeigt werden

  - » Praxis: Thunderbird / Outlook S/MIME-Zertifikat einbinden

E-Mail-Kommunikation verschlüsseln

- PGP (Pretty Good Privacy) ist ein Verfahren zum Verschlüsseln und/oder Signieren von Daten
- PGP erzeugt zwei Teile eines Schlüsselpaares
  - public key (Verschlüsselung)
  - private key (Entschlüsselung)
- Absender, Empfänger und Betreff können nicht verschlüsselt werden
- E-Mail-Text wird mit dem public key des Empfängers verschlüsselt

- Enigmail für Thunderbird
- Gpg4win für Outlook
- GPGTools für Mac

E-Mail-Kommunikation verschlüsseln

- GPG4Win ist eine Sammlung von Programmen:
  - GnuPG
    - die eigentliche Verschlüsselungs-Software.
  - Kleopatra
    - eine einheitliche Benutzerführung für alle kryptografischen Operationen.
  - GNU Privacy Assistent (GPA)
    - eine Alternative zu Kleopatra.
  - GnuPG für Outlook (GpgOL)
    - eine Erweiterung für Microsoft Outlook 2003 und 2007, 2010 und 2013
  - GPG Explorer eXtension (GpgEX)
    - ist eine Erweiterung für den Windows-Explorer
  - Claws Mail
    - ist ein vollständiges E-Mail-Programm mit sehr guter Unterstützung für GnuPG.

E-Mail-Kommunikation verschlüsseln

- Praxis: E-Mail-Kommunikation mit dem Bot Adele

E-Mail-Kommunikation verschlüsseln

1. Mit Kleopatra ein Zertifikat erstellen
2. Zertifikat exportieren (*.asc)
3. Adele anschreiben adele@gnupp.de
   - » Reine Textnachricht mit kopiertem public key
   - » Public key als Anhang
4. E-Mail mit GpgOL entschlüsseln und public key speichern
5. Zertifikat in Kleopatra importieren
6. Fingerabdruck überprüfen
7. Fingerabdruck beglaubigen
8. Signierte E-Mail an Adele senden


Internet Security

Workshop Agenda

- Cyber Security
- System Security
- Data Security
- E-Mail Security
- Internet Security
  - » Web-Browser absichern
  - » Anonym im Internet surfen
- Cyber Defense

Web-Browser absichern

- Plugins nur mit Bestätigung ausführen
- Datenschutz Einstellung
- Verfügbare Plugins verstecken
- Nützliche Erweiterungen – Firefox Add-Ons
  - AdBlock Edge
  - Random Agent Spoofer
  - NoScript

- Praxis: Firefox Security-Tuning in vier Schritten

Anonym im Internet surfen

- Proxy
  - » Proxy bedeutet Stellvertreter und handelt im Auftrag eines anderen
  - » Kann unterschiedliche Netze miteinander verbinden
  - » Kann Netzwerk-Daten filtern, optimieren und zwischenspeichern
  - » Die tatsächliche IP-Adresse des Nutzers bleibt verborgen

  - » Praxis: Firefox Add-on FoxyProxy & Proxy-Listen.de

Anonym im Internet surfen

- Virtual Private Network
  - » Ein virtuelles Netzwerk, welches private Daten über ein öffentliches Netzwerk (z.B. über das Internet) verschlüsselt transportiert
  - » Über eine bestehende IP-Verbindung wird eine zweite Verbindung (Tunnel) aufgebaut
  - » Der gesamte Datenverkehr wird über den VPN-Server geleitet

  - » Tipp: Cisco-VPN der Hochschule in fremden Netzen nutzen (Desktop & Mobil)

Anonym im Internet surfen

- Tor Browser Bundle
  - » Spendenfinanziertes Opensource-Projekt mit über 5000 Tor-Nodes
  - » Komplette Browser Bundles für Windows, Mac OS X, Linux, Android
  - » Zufällige und verschlüsselte Route über drei Tor-Nodes
  - » Jede Note kennt immer nur den Vorgänger und den Nachfolger
  - » Wichtig: nur Anonymisierung, keine Verschlüsselung oder Integritätsschutz

  - » Praxis: Anonym Surfen mit dem Tor Browser Bundle


Cyber Defense

Workshop Agenda

- Cyber Security
- System Security
- Data Security
- E-Mail Security
- Internet Security
- Cyber Defense
  - » Security Awareness
  - » Verteidigungsmaßnahmen

Security Awareness

- Der Mensch als größtes Sicherheitsrisiko
- Know-how der Mitarbeiter
  - » Passwörter wurden nicht geändert, entsprechen nicht den Vorgaben oder sind offen zugänglich
  - » Umgang mit vertraulichen Informationen in der Öffentlichkeit wie z.B. Flughafen Lounge, Flugzeug, Zug, Restaurant, ...
  - » Social Media – Privates und Geschäftliches wird immer mehr vermischt
- Social Engineering, um Menschen gezielt zu manipulieren

Security Awareness

- Hilfsbereitschaft
  - „Ich bin eine neue Studentin, ich muss nur schnell meine E-Mails abrufen."
  - „Könnten sie mir bitte kurz helfen, ich suche Informationen über …."
- Autoritätsgläubigkeit
  - „Ich bin ein Professor aus Sigmaringen und muss schnell an den Rechner."
  - „Ich bin die Sekretärin der Rektorin und brauche heute Abend noch ….."
- Eitelkeit
  - „Ich bin ein Journalist und mache einen Artikel über innovative Studiengänge."
  - „Ich habe ein großes Problem, nur Sie können mir helfen."

Security Awareness

- Neugierde
  - » Öffnen von Attachments, Klicken auf Links, zufällig gefundene DVDs oder USB-Sticks, kostenlose Software, ...
- Einschüchterung
  - » Phishing E-Mail: „Wenn Sie nicht Ihr Passwort erneuern, sperren wir Ihren Account“
- Erpressung
  - » Phishing E-Mail: „Wenn Sie nicht Ihr Passwort erneuern, erheben wir eine Gebühr von 15 Euro ...“

Security Awareness

- Legitimation
  - „Ich habe gerade mit ihrer Kollegin Jessica gesprochen und sie hat gesagt, sie können mir weiterhelfen …“
  - „Ich habe ihren Vorgesetzten, Herrn Müller auf einem Workshop getroffen. Ich weiß, dass er jetzt im Urlaub in Neuseeland ist. Er hat mir versichert, sie können mir helfen …..“
  - „Ich hab vorhin beim Zusammenpacken nach der Präsentation aus Versehen diesen Adapter eingesteckt. Kann ich ihn kurz wieder zurückbringen, ich möchte keinen Ärger bekommen.“
  - „Ich habe gerade eigentlich noch Vorlesung bei Herrn Müller, da ist mein Notebook noch drin, kann ich mal kurz an den Rechner …“

Security Awareness

- Maßnahmen
  - Sensibilisierung und Befähigung der Mitarbeiter
  - Stärken und Schwächen der Mitarbeiter als Tatsache akzeptieren (z.B. Hilfsbereitschaft = Kundenfreundlichkeit)
  - Verhaltensmaßnahmen anbieten und schulen: Ablehnen mit Gegenangebot, Firmenrichtlinie als Verteidigung, ...
  - Aufzeigen und Demonstrationen von möglichen Angriffen
  - Zentrale Position im Unternehmen schaffen, an die „dubiose" Anfragen weitergegeben werden können

Verteidigungsmaßnahmen

- Aktuelle Updates und Sicherheitspatches installieren
  - » Laut Microsoft erfolgen 60% aller Angriffe über bereits geschlossene Lücken
- Veraltete, unsichere und unbenutzte Software deinstallieren
- Restriktive Konfigurationen, eingeschränkte Benutzerkonten
- Sicherheits-Software verwenden (Virenscanner, Firewall, ...)
- Automatische Datensicherungen
- Daten verschlüsseln (früher nur sensible ...)
- Diversifikation (unbekanntere Software nutzen)
- Protokollierung

Verteidigungsmaßnahmen

- Man muss abschätzen, in wie weit sich der „Aufwand“ lohnt
  - » Social Engineering betreiben
    - › Welche Accounts finde ich von mir, wenn ich „google“?
    - › Wie hoch ist die Passwortwiederholung?
- Paranoide Lebensweise ist nicht notwendig
  - » Wie interessant sind meine Daten für eine Person x?
    - › Welche Konsequenz hat es, wenn mein E-Mail-Account bzw. Facebook gehackt wird?
- Praxis: Informationen sammeln und auswerten


Fragerunde

Vielen Dank!

http://cyber-security-workshop.de