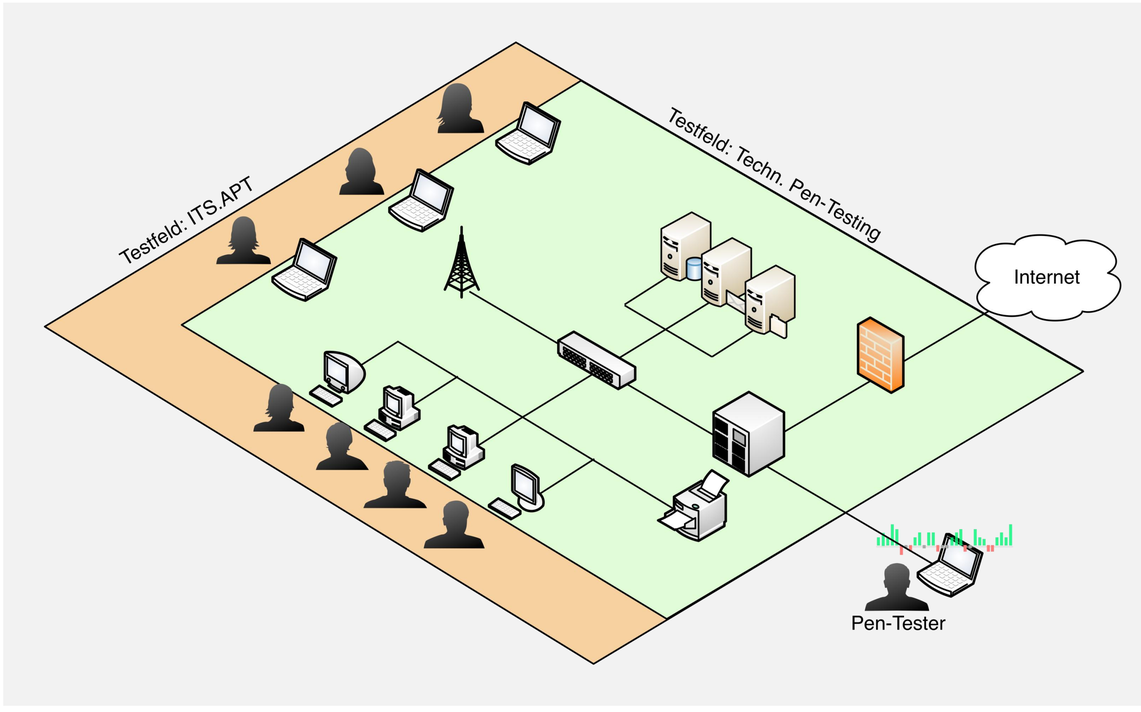
ITS.APT

IT-Security Awareness Penetration Testing

1. THEMA

Angriffe auf IT-Infrastrukturen werden immer häufiger, da sie mit vergleichsweise geringem Aufwand über das Internet möglich sind und die Identität eines Angreifers leicht verschleiert werden kann. Ob der Angriff Erfolg hat, entscheidet oft das individuelle Verhalten der IT-Benutzer, die sich mit einer solchen Attacke konfrontiert sehen. Zur Frage, ob und in welchem Maße das Sicherheitsbewusstsein von IT-Benutzern den Ausgang sicherheitsrelevanter Vorfälle beeinflussen kann, liegen jedoch nur wenige empirische Daten vor. Die Datenerhebung ist nicht nur mit hohen Kosten verbunden, sondern kann auch datenschutz- und arbeitsrechtlich problematisch sein.

Eine Bewertung der IT-Sicherheit bei Betreibern kritischer Infrastrukturen wird üblicherweise durch klassisches „Penetration Testing“ durchgeführt. Bei diesem Vorgang wird die IT-Infrastruktur eines Unternehmens auf Verwundbarkeiten überprüft. Dabei ist das Testfeld jedoch lediglich auf die technische Infrastruktur beschränkt und lässt den Faktor Mensch bei der IT-Sicherheitsbewertung außen vor.



Das Testfeld des klassischen Pentesting wird um den Faktor Mensch erweitert.

2. ZIELE + VORGEHEN

Das Verbundprojekt „IT-Security Awareness Penetration Testing (ITS.APT)“ adressiert derartige Schwierigkeiten mit dem Ziel, diese klassische Methode um den Faktor Mensch zu erweitern, d.h. die Benutzer der IT-Infrastruktur. Im Projekt werden neue Methoden erarbeitet, mit denen IT-Sicherheitsbewusstsein von Benutzern gemessen werden kann. Inwieweit das Sicherheitsbewusstsein von Individuen eine Rolle bei Angriffen auf die IT-Infrastruktur spielt, konnte mit traditionellen wissenschaftlichen Messwerkzeugen bisher nicht praktikabel nachgewiesen werden. Mit einem im Projekt zu definierenden einfach quantifizierbaren Indikator „IT-Sicherheitsbewusstsein“ ließe sich, zum Beispiel im Hinblick auf Kosten und zeitlichen Erhebungsaufwand, wesentlich einfacher arbeiten.

In einem umfassenden Feldtest mit anschließender Evaluation in einem der größten europäischen Zentren für medizinische Versorgung, dem Universitätsklinikum Schleswig-Holstein, wird untersucht, welche Parameter entscheidend für das IT-Sicherheitsbewusstsein der Nutzer sind. In dieser Umgebung sind die Auswirkungen sicherheitsrelevanter Vorfälle besonders gravierend und die Anforderungen an den Datenschutz besonders hoch.

3. DIE PARTNER

ULD – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

UKSH – Universitätsklinikum Schleswig-Holstein

Universität Duisburg Essen

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

universitätbonn

ERNW providing security.

Westfälische Wilhelms-Universität Münster

4. HUMAN PENTESTING

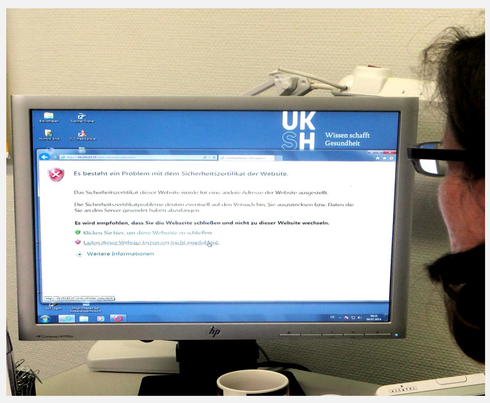
Der Faktor Mensch: Im Rahmen des Projekts werden die psychologischen Grundlagen erarbeitet um zu verstehen in wie weit IT-Security-Awareness den Menschen in seinem Handeln beeinflusst.

Juristische Implikationen: Es wird analysiert in welchem Rahmen Awareness-Pentesting im laufenden Betrieb umsetzbar ist und es werden konkrete Handlungsempfehlungen für eine Umsetzung erarbeitet.

Datenschutzgrundsätze: Die Privatsphäre der Mitarbeiter von Unternehmen darf durch Awareness-Pentesting nicht empfindlich gestört werden. Es werden Grundsätze entwickelt um dies zu gewährleisten.

Industrielles Pentesting: Das industrielle Pentesting kann mit den Ergebnissen von ITS.APT systematisch um die *menschliche Komponente* erweitert werden.

Technische Umsetzung und Metriken: Eine prototypische Umsetzung erlaubt die Messung von IT-Security-Awareness und damit auch eine gezielte Schulung sowie Bewertung dieser Maßnahmen.



Eine Sicherheitswarnung des Browsers kann auf einen Angriff auf die IT-Infrastruktur hinweisen. Jetzt entscheidet die Reaktion des Nutzers über den Erfolg des Angriffs.
(Quelle: UKSH).

Eine Mitarbeiterin des UKSH wird bei ihrer alltäglichen Arbeit Zeuge eines IT-Sicherheitsvorfalls.

5. INNOVATION + PERSPEKTIVE

Die angestrebte Innovation umfasst ein Werkzeug zur kosteneffizienten Messung des kollektiven IT-Sicherheitsbewusstseins ganzer Unternehmen und bietet damit neue Erkenntnisse für alle beteiligten Forschungsbereiche: Rechtswissenschaften, Psychologie und Informatik. Auch das IT-Risikomanagement von Unternehmen kann so verfeinert werden. Zudem werden neue Ansätze zur Erhöhung des IT-Sicherheitsbewusstseins der Nutzer geschaffen und exemplarisch im Rahmen des Projekts umgesetzt.

ITS.APT

Kontakt:
Prof. Dr. Michael Meier & Arnold Sykosch
Institut für Informatik 4, Arbeitsgruppe IT-Sicherheit
Rheinische Friedrich-Wilhelms-Universität Bonn
Friedrich-Ebert-Allee 144, 53111 Bonn
https://itsec.cs.uni-bonn.de/itsapt
its.apt@uni-bonn.de