Kurzbeschreibung

„Live-Hacking“

Inhalt

1. Über secunet

secunet ist einer der führenden deutschen Anbieter für anspruchsvolle IT-Sicherheit. Mehr als 400 Experten konzentrieren sich auf Themen wie Kryptographie, E-Government, Business Security und Automotive Security und entwickeln dafür innovative Produkte sowie hochsichere und vertrauenswürdige Lösungen. Zu den mehr als 500 nationalen und internationalen Kunden gehören viele DAX-Unternehmen sowie zahlreiche Behörden und Organisationen. secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

secunet wurde 1997 gegründet und erzielte 2016 einen Umsatz von ca. 115 Millionen Euro. Die secunet Security Networks AG ist im Prime Standard der Deutschen Börse gelistet.

2. Leistung

Informationssicherheit entsteht nicht einfach nur durch technische Maßnahmen. Vielmehr ist Informationssicherheit ein Prozess, der gelebt werden muss. Führungskräfte spielen in diesem Ablauf ebenso eine entscheidende Rolle wie jeder einzelne Mitarbeiter und die IT-Abteilung. Im Idealfall richten Führungskräfte ihre Entscheidungen an der Informationssicherheit aus und motivieren die Mitarbeiter durch ihre Vorbildfunktion, das Thema Informationssicherheit zusammen zu leben. Die IT-Abteilung setzt Maßnahmen zur Unterstützung der Mitarbeiter um und jeder einzelne Mitarbeiter verhindert IT-Sicherheitsvorfälle durch sein bewusstes Handeln.

Die reine Vermittlung von Informationen hat in den letzten Jahren nur sehr partiell dazu geführt, dass Anwender beispielsweise „gute“ Passwörter verwenden. Das zeigt, dass sich bisher immer noch kein ausreichendes Sicherheitsbewusstsein für digitale Medien etabliert hat. Um Interesse für das Thema zu wecken und jedem einzelnen zu demonstrieren, dass er für die IT-Sicherheit mitverantwortlich ist, bieten wir einen lebendig gestalteten Live-Hacking-Vortrag an. Themen der Informationssicherheit bereiten wir humorvoll auf und machen sie in konkreten Szenarien für die Zuhörer so präsent, dass diese die Probleme wirklich verstehen und ein nachhaltiges Bewusstsein für das Thema entwickeln – wie uns das Feedback nach solchen Vorträgen bestätigt.

Die Performance führen wir immer zu zweit oder zu dritt in einer Art Rollenspiel durch. Anhand einer Geschichte werden die Probleme live aufgezeigt und vorgeführt. Entscheidend ist die direkte Darstellung der Gegenmaßnahmen, beziehungsweise die Anleitung zum korrekten Vorgehen. Es soll nicht einfach nur geschockt werden.

Der Vortrag kann als eine Art Initialzündung für das Thema im Haus herangezogen werden, zur Auffrischung des Themas dienen oder auch, mit Schulungsinhalten verknüpft, konkrete Lehrinhalte transportieren.

2.1. Inhalt und Ablauf

Zeitrahmen:
Von 20 bis 180 Minuten ist alles möglich, abhängig von den Inhalten und Ihren Vorstellungen.

Inhalte:
Die folgenden Themenblöcke geben einen Überblick von möglichen Themen. Die Ausprägung ist dabei sehr unterschiedlich und sollte vorab in einem Gespräch geklärt werden:

- Mobile Sicherheit
  - Angriffe auf Smartphones (Trojaner, Apps, Zugriffsschutz)
  - WLAN-Angriffe
  - Angriffe auf mobile Datenträger
  - Bluetooth-Angriffe
- Passwortsicherheit
  - Angriffe einfache Passwörter
  - Problemstellung einfache Passwörter
  - Angriffsvariationen auf Zugangsdaten Internet/Intranet
- Trojaner und Malware
  - Angriffe auf Windows-Systeme mit Übernahme der Computer
  - Phishing/Pharming
- Systemsicherheit
  - Umgehung von Anmeldepasswörtern
  - Angriffe auf bereits eingeschränkte Systeme
  - Erlangen von Adminrechten
  - Angriffe über intelligente Peripheriegeräte (Teensy)
- Websicherheit
  - Cross-Site-Scripting
  - Sicherheitslücken in CMS-Systemen
- Dokumentensicherheit
  - Angriffe auf Word und PDF
  - Umgang mit Dokumenten
- Soziale Netze
  - Beispiele für Social Engineering

Natürlich sind weitere Szenarien möglich und zusätzliche Schulungsinhalte können flexibel erstellt werden. Sprechen Sie uns gern direkt an.

3. Die Referenten

Marian Jungbauer ist seit Februar 2012 bei secunet. Vorrangig wird er gefragt für Penetrationstests bei Behörden und Firmen. Zuvor war er Projektleiter im Bereich Trusted Desktop bei der Sirrix AG. Von Oktober 2007 bis Anfang 2011 arbeitete er am Institut für Internet-Sicherheit an der Fachhochschule Gelsenkirchen als wissenschaftlicher Mitarbeiter und war Projektleiter im Bereich Trusted Computing und technischer Projektleiter im Bereich Awareness. Mit dem Awareness-Schulungskonzept ist er als Mitentwickler seit einigen Jahren bei vielen Veranstaltungen und Kongressen als Vortragender zu Gast. Er hat das Studium der Informatik an der FH Gelsenkirchen im Bereich Trusted Computing mit dem Diplom abgeschlossen und ist Autor einer Vielzahl von Veröffentlichungen.

Markus Ohnmacht arbeitet seit September 2012 bei secunet. Seine Aufgaben umfassen die Bereiche Informationssicherheitsmanagementsysteme und Awareness außerdem ist er in der Produktentwicklung von secunet safe surfer tätig. Vor der Zeit bei secunet hat er zunächst eine Ausbildung zum Fachinformatiker – Systemintegration und anschließend ein Studium „Security Management“ absolviert. Markus Ohnmacht ist aktiv für das secunet Hacker-Team im Einsatz und hat bereits zahlreiche Live-Hackings bei großen Unternehmen und Behörden durchgeführt.

Anne Lahner ist bereits seit 1999 bei secunet und damit in der IT-Sicherheitsbranche unterwegs. Aus ihrer Erfahrung in Awareness- bzw. Sensibilisierungsprojekten kennt sie die kleinen menschlichen Schwächen in Bezug auf die Informationssicherheit. Sie versteht sich als Schnittstelle zwischen Technikabteilung und Anwendern – und kann technisch anspruchsvolle Sachverhalte verständlich und ohne Fachchinesisch erklären. Anne Lahner arbeitet mit den ethischen Hackern und Pentestern von secunet zusammen und ist aktiv mit dem secunet Hacker Team quer durch die Republik unterwegs.

Robert Fritzen arbeitet seit 2015 bei secunet und ist als Berater für Informationssicherheit im Bereich Pentest und Forensik aktiv. Neben Live-Hackings gehören IT-Sicherheitsanalysen und Penetrationstests zu seinen hauptsächlichen Tätigkeiten. Vor der Beratertätigkeit war er im Forschungsbereich Botnetze des Instituts für Internet-Sicherheit der Westfälischen Hochschule tätig. Robert Fritzen veröffentlichte für verschiedene Fachzeitschriften u.a. zum Thema Abwehr von DDoS-Angriffen und schloss sein Masterstudium im Bereich IT-Sicherheit zum Thema Intrusion-Alert-Korrelation ab.

Markus Stark arbeitet seit 1997 für die secunet. Zuvor war er nach seinem Informatik-Studium an der Universität Dortmund als Entwickler und IT-Sicherheits-Berater für den TÜViT tätig. So führte er schon 1995 Penetrationstests bei Banken durch. In den langen Jahren bei der secunet war er in vielen verschiedenen Bereichen national und international tätig. Zurzeit liegen seine Schwerpunkte in der Beratung und Erstellung von Sicherheitskonzepten für Behörden und Unternehmen mit hohen Sicherheitsanforderungen und Verschlusssachenbearbeitung.

Michael Lamberty ist seit 2016 ein secunet-Pentester im Bereich Kritische Infrastrukturen. Zuvor studierte er den Master Internet-Sicherheit an der Westfälischen Hochschule (ehemals FH) Gelsenkirchen und war Mitarbeiter beim Institut für Internet-Sicherheit, seine Masterarbeit fertigte er in Kooperation mit dem Antiviren-Hersteller IKARUS in Wien an, wo er Beiträge zur Malware-Erkennung auf Android-Geräten leistete.

Kevin Ott ist seit 2016 als Berater für Informationssicherheit und Penetrationstester für die secunet beschäftigt. Vor seiner Zeit bei der secunet arbeitete er als Technical Analyst im Network Security Engineering der Deutschen Bank AG. Als Ethical Hacker untersucht er Systeme und Infrastrukturen von Unternehmen aus der Wirtschaft und Behörden auf Schwachstellen. Zu seinen bisherigen Erfahrungen zählen Webanwendungen, Windows Systeme, WLAN Architekturen und NAC Lösungen. Er verfügt außerdem über Erfahrungen mit ICS Systemen und ist ein aktives Mitglied des Live-Hacking Teams der secunet.

Felix von Eye arbeitet seit September 2016 bei secunet. Zu seinen Aufgaben gehört neben allgemeiner IT-Sicherheitsberatung das Erstellen von technischen Richtlinien. Zuvor war er seit 2009 als wissenschaftlicher Mitarbeiter in diversen Forschungsprojekten in verschiedenen Themenbereichen der IT-Sicherheit angestellt. Im Zuge der Forschungsprojekte veröffentlichte Felix von Eye ein Buch und eine Vielzahl an Veröffentlichungen unter anderem in Fachzeitschriften und hielt wissenschaftliche und technische Vorträge im deutschsprachigen und europäischen Raum.

Sebastian Halle ist seit August 2016 als Berater für Informationssicherheit bei secunet. Zu seinen Aufgaben gehören u.a. die Erstellung von Sicherheitskonzepten nach BSI-Grundschutz, die Mitwirkung bei IT-Sicherheitsanalysen und die Durchführung von Kurzrevisionen, in Anlehnung an die IS-Kurzrevision des BSI, im behördlichen Umfeld.

Vor der Zeit bei secunet war der gelernte Fachinformatiker und geprüfte IT-Berater zwischen August 2006 und August 2016 als IT-Administrator, IT-Consultant, IT-Sicherheitsbeauftragter und IT-Ausbilder für eine mittelständische Unternehmensgruppe aus Gelsenkirchen tätig. Er bringt Projekt-Erfahrungen aus den unterschiedlichsten Branchen mit. Seit Februar 2017 ist er für das secunet Hacker-Team aktiv im Einsatz.

Markus Linnemann ist Leiter der Division Kritische Infrastrukturen und seit Juni 2011 bei secunet. Zuvor war er ab Juli 2008 Geschäftsführer des Instituts für Internet-Sicherheit der FH Gelsenkirchen. Mit seinen Kollegen entwickelte er erfolgreich ein neues Geschäftsfeld und etablierte Live-Hacking-Veranstaltungen, die mittlerweile bei vielen öffentlichen und privatwirtschaftlichen Auftraggebern durchgeführt werden. Vor seiner Ernennung zum Geschäftsführer arbeitete er von Juli 2005 bis Juni 2008 am Institut als Projektleiter in den Bereichen Trusted Computing, Identity Management und Awareness. Seine Diplomarbeit in Informatik an der FH Gelsenkirchen verfasste er zum Thema Identity Management. Markus Linnemann ist Autor eines Buches und einer Vielzahl von Veröffentlichungen. Als Experte für das Thema IT-Sicherheit und Security Awareness wird er von Rundfunk, TV und Print-Medien gefragt.

Dirk Reimers arbeitet bereits seit 1999 für secunet. Zuvor hat er den Windows-Bereich im DFN-CERT aufgebaut und technische Vorträge und Tutorien für das DFN-CERT geleitet. Heute leitet er bei secunet das Penetrationstest-und-Forensik-Team und koordiniert die Tätigkeiten der Ethical Hacker. Das Vorgehens- und Dokumentationsmodell von secunet basiert auf seiner langjährigen Tätigkeit. Darüber hinaus analysiert er als aktiver Ethical Hacker intern und extern erreichbare Unternehmensnetzwerke, WLANs und IT-Organisationen. Mehrfach veröffentlichte er Artikel in Fachzeitschriften und wurde als Sicherheitsexperte im Fernsehen zurate gezogen.

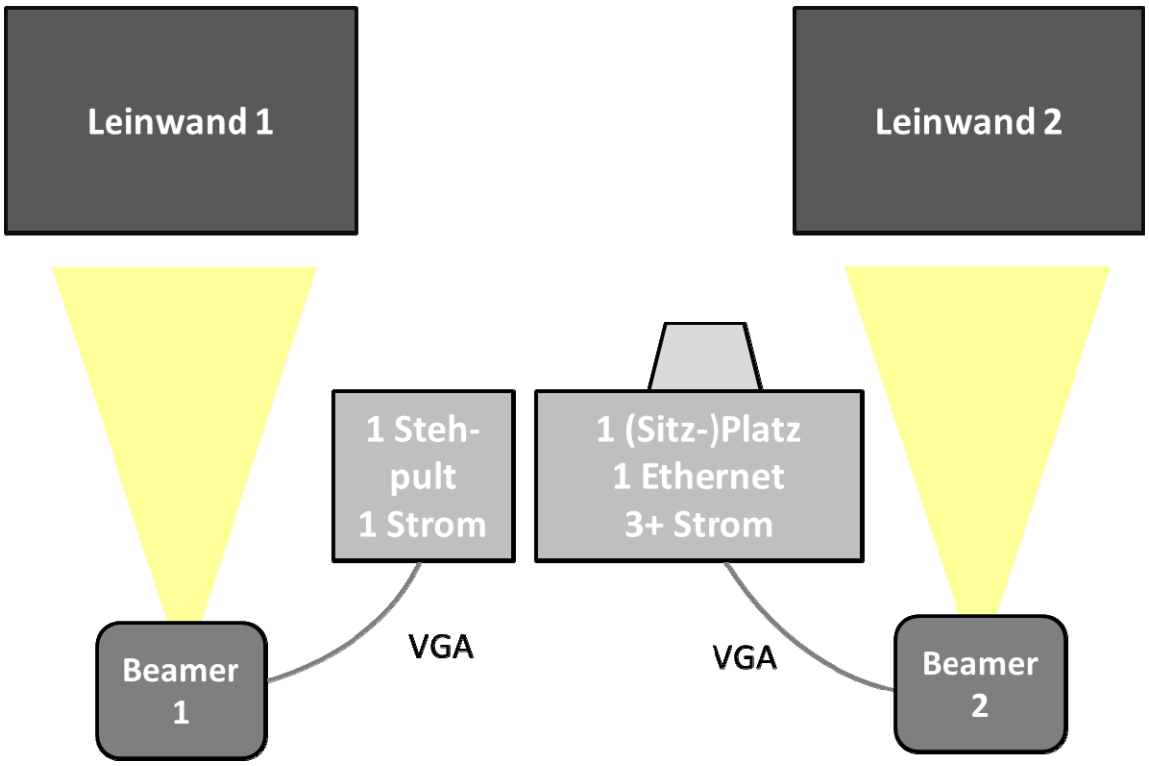
4. Die technischen Voraussetzungen

Für die Durchführung benötigen wir:

- 1 Stehpult/-tisch und ein Sitzplatz mit Tisch
- Stromanschlüsse an Stehplatz und Sitzplatz wie unten beschrieben
- 2 Anzeigegeräte und 2 Anzeigeflächen (2 Beamer, 2 Leinwände oder TFTs, …)
- Anschluss Beamer per VGA (je 1 x am Stehpult, 1 x am Sitzplatz)
- Auflösung Beamer: 1.024 x 768
- 1 Internetanschluss (1 LAN-Kabel) am Sitzplatz (kein WLAN)
- Mobiltelefon-Empfang sollte möglich sein, da sonst nicht alle Szenarien gezeigt werden können (insbesondere Teile des Themenblocks „Mobile Sicherheit“)
- Ab ca. 50 Personen evtl. ein Soundanschluss, 3,5 mm Klinke
- Bitte Headsets als Mikrofone
- Notebooks und weiteres Equipment werden von uns bereitgestellt.
- Bereitstellung der u.g. Ausstattung bitte bis eine Stunde vor Veranstaltungsbeginn
- Wenn möglich, stilles Wasser für die Referenten

Film- und/oder Tonaufnahmen bitte nur nach vorheriger Absprache!

Schematischer Aufbau:



5. Referenzen

Wir waren mit unserem Konzept schon bei weit über 100 Behörden und Unternehmen im Einsatz. Beispiele:

- Bundesministerium für Wirtschaft und Technologie (explizit Führungskräfte, auch Staatssekretäre)
- Bundesministerium des Innern
- Bundesministerium für Familie, Senioren, Frauen und Jugend
- Bundesministerium der Justiz
- Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (explizit Leitung)
- Bundessozialgericht
- Behördenleitertagung der Bundesregierung
- Bundesverwaltungsgericht
- Vodafone
- Deutscher IT-Sicherheitskongress
- Brecko
- ECO
- …

6. Kontakt

Haben Sie Fragen? Besuchen Sie unsere Webseite www.secunet.com/awareness und sprechen Sie uns gern direkt an:

Anne Lahner
Tel.: +49 201 5454 3722
E-Mail: anne.lahner@secunet.com