Area: Allgemeine Diskussion

Hier ist Raum für allgemeine Diskussionen

Area: Informationssicherheit im Homeoffice (Arne Windeler, TU Braunschweig)

Mit der Corona-Pandemie ging es für viele Arbeitnehmende von einem Tag auf den anderen ins Home-Office. Hierbei war an erster Stelle wichtig, dass dort überhaupt gearbeitet werden kann. Leider blieb dabei die IT-Sicherheit an vielen Stellen auf der Strecke. An diesem Punkt setzt der Vortrag „IT-Sicherheit im Home-Office“ an. Er befasst sich damit, was Arbeitgebende zu beachten haben und wie auch die Arbeitnehmenden zur Sicherheit beitragen können.

- Was sollte im Normalfall geklärt werden, bevor im Home-Office gearbeitet werden darf?
- Welche Sicherheitsvorkehrungen sind zu treffen?
- Wie kann der Datenschutz auf dem Weg zwischen Dienststelle und Heimarbeitsplatz gewährleistet werden?
- Wie kann der Datenschutz am Heimarbeitsplatz gewährleistet werden?
- Wie organisiert man sich am besten im Home-Office?

Area: Anatomie eines Sicherheitsvorfalls: Von der Meldung bis zur digitalen Forensik (Pascal Brückner, TU Dresden)

Die Geschichte eines realen Sicherheitsvorfalls an der TU Dresden, der mit einer scheinbar routinemäßigen Meldung begann und ein tiefgreifenderes Problem ans Tageslicht beförderte. Der Vortrag veranschaulicht die Methoden zur Vorfallsbearbeitung in einem CERT (Computer Emergency Response Team) am ganz konkreten Beispiel, um für die Notwendigkeit von Sicherheitsmeldungen auch bei scheinbar unbedeutenden Vorfällen zu sensibilisieren.

Area: Vorsicht Falle! Hacker, Diebe, Social Engineerer (Holger Beck, Universität Göttingen/GWDG)

Social Engineering – eine Modewort für ein ganz altes Phänomen, vielen vielleicht nicht bekannt oder klar, was es bedeutet. Dabei geht es eigentlich nur um die gute (oder in Anbetracht der Ziele schlechte), alte Kunst der Überredung und Verleitung zu für sich selbst schädlichen Handlungen – jetzt eben nur mit moderneren Methoden und Mitteln. Um sich vor solchen Fallen schützen zu können, ist es wichtig , sich bewusst zu sein, welche Methoden Kriminelle heute einsetzen, und eine Orientierung zu haben, wie man solche Angriffsversuche erkennt. Der Vortrag soll für das Problem sensibilisieren, die Bandbreite der Angriffsmethoden beleuchten und anhand von Beispielen verdeutlichen.

Area: Privatsphäre im Netz schützen – das “Best of” der Browser-Erweiterungen (Irmi Blomenkemper, Universität zu Köln)

Beim Vortrag zum “sicheren Surfen” unter Privacy-Aspekten geht es um die Fragen:
Wie kann man „sicher“ surfen, dass möglichst wenig Daten über mich und mein Surfverhalten abfließen?
Was kann ich tun, um trotzdem einigermaßen bequem zu Surfen, ohne von Cookiewarnungen gestört zu werden?
Und nur als Randthema (da es hierbei nicht hauptsächlich um ein Privacythema, sondern mehr um Maßnahmen zur Schonung der eigenen Nerven handelt): Wie kann ich Werbung auf Webseiten wirkungsvoll blockieren

Außerdem werden einige häufig eingesetzte Browser-Erweiterungen (AddOns) vorgestellt, die hilfreich beim Löschen von Cookies sind, beim Blockieren von Werbung unterstützen oder vor heimlich im Hintergrund mitanalysierenden Drittanbietern schützen.

Area: APT aus Sicht des Angreifers (Marius Mertens, Uni Duisburg-Essen)

Der Vortrag “APT aus Sicht des Angreifers” zeigt Motivation und Methoden, warum und wie Angreifer versuchen, Rechnersysteme für ihre Zwecke zu übernehmen. Dabei sind nicht nur große Unternehmen oder Regierungsnetze betroffen, sondern auch einzelne Anwender geraten ins Visier – ob absichtlich oder als Kollateralschaden. Mit der Darstellung der Angreiferperspektive wollen wir dazu motivieren, die eigenen Sicherheitsmaßnahmen zu hinterfragen und zu optimieren.

Area: Die 4×4 der verbreitesten IT-Sicherheitsirrtümer (Christian Böttger, TU Braunschweig)

Angelehnt an eine Auflistung des Bundesamts für Sicherheit in der Informationstechnik (BSI) behandeln wir heute die jeweils vier wichtigsten Irrtümer zu Informationssicherheit aus den Bereichen “**Surfen im Internet**“, “**E-Mail-(Un)Sicherheit**“, “**Mobile Geräte**” und “**Computer / PC-Sicherheit**”

Area: Guided Tours der Online Dienste des GITZ (Leonard Jari Zurek, TU Braunschweig)

Wir stellen Ihnen die verschieden Online-Dienste des GITZ vor und zeigen Ihnen, wo sie weitere Informationen zur Informationssicherheit finden.

Area: Die 11 “Goldenen Regeln” der IT-Sicherheit (Christian Böttger, TU Braunschweig)

Wir zeigen Ihnen, welche 11 (einfachen) Punkte Sie beachten sollten, um ein Grundniveau an Informationssicherheit an Ihrem Arbeitsplatz und zu Hause zu erreichen.

Area: Tücken des Alltags (Bernhard Brandel, KU Eichstätt-Ingolstadt)

Nicht nur in Studium und Beruf, sondern auch im alltäglichen Leben besitzen wir Informationsschätze, für die sich Dritte ungefragt interessieren.

Wie schützen wir auch außerhalb des Berufs unsere wichtigen Informationen? Was können wir methodisch aus den Situationen an der Hochschule in den Alltag übertragen?

Mit diesen Fragen beschäftigen wir uns in diesem Vortrag, gewürzt mit zahlreichen typischen und weniger typischen Beispielen aus dem Alltag, der Welt und dem Internet der Dinge.

Area: (Un-)Sichere Passwörter (Christian Böttger, TU Braunschweig)

- Warum Passwörter?
- Wie wähle ich ein sicheres Passwort?
- Wie bewahre ich Passwörter auf?

Area: Emotet/Trickbot – Ein Fallbeispiel für Bedrohungen (Christian Böttger, TU Braunschweig)

Die allgegenwärtige Bedrohung durch Spam/Phishing-Mails bekommt eine neue Dimension. „Emotet“ kombiniert die Methode der Spamverteilung „Spear-Phishing mit Methoden des Social Engineering“ mit gefährlicher Schadsoftware (Advanced Persistent Threats APT). Mittlerweile – nach “Abschalten” von Emotet – tritt “Quakbot” verstärkt auf. Die Bedrohung ist ähnlich gefährlich und auch technisch verwandt.

Nach der Infektion eines Zielsystems ist Emotet in der Lage, das Outlook-Addressbuchs des Opfers auszulesen und sich selbst per Spear-Phishing weiter zu verbreiten. Neuerdings liest es auch die E-Mails des Opfers (Outlook-Harvesting) und nutzt die Inhalte, um authentisch aussehende Spear-Phishing-Mails zu erzeugen (Social Engineering). Dann verschickt es im Namen des Opfers über dessen echte E-Mail-Adresse sich selbst an die gespeicherten Kontakte.

Darüber hinaus ist Emotet in der Lage, weitere Schadsoftware je nach Bedarf und Absicht des Angreifers nachzuladen und sich dadurch dauernd zu verändern. Beobachtet wurden bisher insbesondere, aber nicht nur, die Banking-Trojaner „Trickbot“ sowie „Quakbot“. Diese können sich selbstständig von einem infizierten Rechner als Wurm im befallenen Netzwerk weiter ausbreiten, auch ohne den weiteren Versand von Spam-Mails.

Die Schadprogramme werden aufgrund ständiger Modifikationen zunächst meist nicht von gängigen Virenschutzprogrammen erkannt und nehmen tiefgreifende Änderungen an infizierten Systemen vor.

Ein einzelner infizierter Rechner kann somit das komplette Netzwerk einer Organisation infizieren und lahm legen. Es sind bereits mehrere solcher Vorfälle öffentlich bekannt geworden, beispielsweise die Universität Gießen. Gefährdet sich besonders Umgebungen, die zentralisierte Windows-Systeme einsetzen.

Area: E-Mail-Sicherheit / Phishing (Christian Böttger, TU Braunschweig)

- E-Mail-Gefahren durch Phishing: Überblick und was ist das?
- Verschiedene Vorgehensweisen der Angreifer
- Mögliche Ziele der Angreifer
- Verschiedene Angriffstypen und ihre Auswirkungen
- Schutzmaßnahmen: was können Sie dagegen tun?
    - mit realen Beispielen
    - Informationsquellen für weitergehende Informationen

Area: Informationssicherheit für Zuhause – Tipps&Tricks für die Heimnetzsicherheit (Leonard Jari Zurek, TU Braunschweig)

Viele Dienste sollen heutzutage “einfach funktionieren”, für Heimnetzgeräte bedeutet dies oft “plug and play”. Doch oftmals hilft es, sich mit der Technik etwas weiter auseinanderzusetzen, um sowohl Sicherheitsrisiken zu minimieren, als auch die generelle Leistung zu verbessern. Sei es das Einrichten von 2FA, WLAN-Passwörter, Gästenetzen, oder Nutzungsbeschränkungen, viele Heimnetzgeräte liefern deutlich mehr Möglichkeiten als jene, die standardmäßig benutzt werden. In diesem Vortrag werden einige Hinweise, Tipps und Tricks zur Verbesserung der Sicherheit im Heimnetz vorgestellt.

Area: Messenger – Datenschutz und Informationssicherheit (Holger Beck, Universität Göttingen/GWDG)

WhatsApp, Signal, Telegram, Threema und andere Messenger-Dienste werden von Milliarden von Nutzern eingesetzt. Schneller und bequemer Austausch von Nachrichten, Bildern, Videos und Dateien und meist auch gute Erreichbarkeit von Kommunikationspartner tragen dazu bei, dass niemand mehr auf solche Dienste verzichten möchte. Für Skeptikern kommt der Druck hinzu, mitmachen zu müssen, um nicht im Abseits zu stehen.

Der Beliebtheit gegenüber stehen Fragen zu Datenschutz und Informationssicherheit der Messenger. Die Diskussionen gehen hier manches Mal hoch her, wobei viele Meinungen nicht immer zu mehr Klarheit beitragen. Der Vortrag soll positive wie negative Aspekte für Datenschutz und Informationssicherheit aufarbeiten und damit dazu beitragen, Risiken und Chancen besser einzuschätzen und Messenger angemessen zu nutzen (oder auch einmal darauf zu verzichten).

Area: Sicherheit im WLAN (Steffen Klemer, GWDG)

Mit unsere Handys, Tablets und Laptops sind wir heute fast durchgängig ‘on’. Irgendwo das Gerät aktiviert, kann fast überall sogleich eine WLAN-Verbindung aufgebaut werden und die Daten können frei aus der und in die weite Welt sausen. Wie erreicht wird, dass auch ohne ein schützendes Kabel als Transportmedium, die Daten sicher sind, soll hier beleuchtet werden. Ein besonderer Fokus liegt auf den Aspekten, die dabei schief gehen können und wie man sich davor schützen kann.

Area: Cyber-Security-Escape-Room *Anmeldung erforderlich (Eric Lanfer, René-Maximilian Malsky, Uni Osnabrück)

Lernen Sie spielerisch die wichtigsten Grundlagen der IT-Sicherheit in einem Escape Game. Tauchen Sie dabei in die Rolle eines/einer Angreifer*in ein und verschaffen Sie sich Zugang zu betriebsinternen Dokumenten. Für diese Veranstaltung sind keinerlei Vorkenntnisse notwendig. Da die Kapazitäten beschränkt sind, ist für diese Veranstaltung eine Anmeldung erforderlich. Schicken Sie dazu bitte eine formlose E-Mail mit Ihrem Namen an ecsm@uos.de

Area: Podiumsdiskussion

Abschlussgespräch in Form einer moderierten Podiumsdiskussion mit ausgewählten Referent*innen der IT-SAD.