

Computernetzwerke und IT-Sicherheit

Wochenendseminar im Aura-Hotel Saulgrub vom 2. bis 4.10.2015

1. Überblick

Computer sind aus unserer heutigen Welt nicht mehr weg zu denken. Sie steuern und regeln zahllose Prozesse in fast allen Geräten der Unterhaltungselektronik, Haushaltstechnik, PCs, Telefonanlagen, Autos und Smartphones, die heute in einem normalen Haushalt zu finden sind. Sie entfalten ihren vollen Nutzen, wenn sie miteinander verbunden werden, also vernetzt sind. Diese Vernetzung von Computern bringt für den Anwender viele Vorteile und Annehmlichkeiten, ist aber auch mit Risiken verbunden, die er kennen sollte.

Da das Verständnis von Computernetzwerken von grundlegender Bedeutung für die Beurteilung der daraus entstehenden Bedrohungen ist, befaßt sich dieses Seminar im ersten Drittel mit dem strukturellen Aufbau und der Funktionsweise dieser Netze. Aus welchen Komponenten bestehen sie, wo liegen die Schwachstellen und was muß alles durch den Computer gemacht werden, damit man im Internet surfen oder eine Banküberweisung machen kann.

Wenn die groben technischen Zusammenhänge bekannt sind, kann man besser verstehen, wie dieses 'Nervensystem' unserer modernen Gesellschaft angegriffen werden kann und wie man sich dagegen wirksam schützt. Das Fachgebiet, das sich mit diesen Fragen befaßt, heißt IT-Sicherheit und ist Gegenstand des zweiten Drittels dieses Seminars. Im letzten Teil wird die Sicherheit beliebter Netzdienste und Cloudanwendungen betrachtet, bevor konkrete Tipps für einen sicheren Umgang mit den modernen Medien gegeben werden.

Abgrenzung, wichtig:

Das Seminar wendet sich ganz allgemein an alle Benutzer von Computern, unabhängig vom benutzten Betriebssystem und versucht daher Hersteller- und Systemunabhängige Informationen und allgemeingültige Tipps zu geben. In der Kürze der Zeit ist es nicht möglich, auf spezielle Windows-Problematiken und ihre Zusammenhänge mit individuell genutzten Blindenhilfsmitteln einzugehen. Dies kann nur in einer individuellen Schulung vor Ort beim Computeranwender erfolgen!

2. Zielgruppe

Zielgruppen sind beruflich oder auch privat interessierte blinde, sehbehinderte und sehende Personen, die mehr über Computernetze, ihre Funktionsweise, Chancen und Risiken dieser Technologie, sowie wirksame Schutzmaßnahmen aus dem Bereich der IT-Sicherheit erfahren möchten. Das Verständnis für das Spannungsfeld der IT-Sicherheit zu fördern und die Zusammenhänge zwischen unendlichen Möglichkeiten und andererseits stetig wachsender Bedrohungen durch diese Technologie transparent zu machen und entsprechend zu sensibilisieren, sind weitere Ziele dieses Seminars.

3. Methodik

Die einzelnen Themenblöcke sind als freier Vortrag mit zum Teil visueller Unterstützung durch Textprojektion konzipiert. Die wichtigsten Sachverhalte werden detailliert erklärt und durch Übungen vertieft. Jeder Teilnehmer erhält eine CD mit Themenbeschreibungen und Tipps zu Internetquellen.

4. Agenda

4.1 - Tag 1, Freitag 2.10.2015

17:30 Uhr - Abendessen, Seminarbeginn

19:00 Uhr - Begrüßung, Vorstellung der Seminarteilnehmer und Agenda.

19:30 Uhr - Block 1 - Einführung und Netzwerkgrundlagen

Teil 1 - Die Allgegenwärtigkeit von Computern und ihren Kommunikationsnetzen. Wo finden wir Computer, wie tauschen sie Daten aus und was ist der Nutzen dieser globalen Informationsströme? Computer steuern heute praktisch alle Prozesse, auf die eine moderne Gesellschaft angewiesen ist. Die Palette reicht hierbei von Maschinen und Geräten der Haustechnik, der Unterhaltungselektronik, dem Zahlungsverkehr bei Banken, in der Logistik, bei Werkzeugmaschinen und Robotern in der Industrie, über die Wasser und Stromversorgung bis hin zu medizinischen lebenserhaltenden Spezialsystemen in Krankenhäusern. Überall werden elektronische Geräte mit sogenannten Steuereinheiten miteinander vernetzt, um einen maximalen Nutzen zu erreichen. Da die Vernetzung dieser verschiedenen

Computersysteme auf vielfältige Weise erfolgen kann, wird sich dieses Seminar inhaltlich auf die heute gebräuchlichste Form TCP/IP basierender Netzwerke konzentrieren.

Teil 2 - Geschichte der Computer und die Anfänge des Internets. Was heute als Internet bekannt ist und rund 3 Milliarden Menschen weltweit miteinander verbindet begann vor 45 Jahren mit 4 Großrechnern in Los Angeles. Es ist eine Erfolgsgeschichte ohne Beispiel, die eine endlose Reihe von Erfindungen und Entwicklungen umfaßt und durch einige glückliche Umstände zu dem geführt hat, was wir heute alle tagtäglich wie selbstverständlich benutzen. Trotzdem sollte der Nutzer des Internets sich bewußt sein, daß dieses gesamte riesige Netzwerk nie für den Zweck entwickelt wurde, für den wir es heute einsetzen!

Teil 3 - Warum ist das Internet heute so extrem wichtig? Szenarien, was passiert wenn?

Teil 4 - Was benötigt man für ein kleines Netzwerk? Praxisteil zum Kennenlernen einfacher, privat nutzbarer Netzwerkkomponenten.

21:00 Uhr - Ende Tag 1

4.2 - Tag 2, Samstag 3.10.2015

09:00 Uhr - Block 2 - Das Internet, größtes Computernetz der Welt

Teil 1 - Aufbau und Struktur des Internets. Was ist ein Server und was ein Client? Was sind Router, Switches, WEB-, Mail-, File-, Datenbank- und Nameserver und welche Aufgaben sollen sie erfüllen? Wie müssen Informationen verpackt werden, damit sie die lange Reise vom Sender zum Empfänger im Internet unbeschadet überstehen? Was muß der Computer tun, damit er ein vollwertiger und akzeptierter Teilnehmer im Internet ist?

Teil 2 - Das ISO-OSI Schichtenmodell. Es ist die biblische 7, die zur Strukturierung der komplexen Vorgänge bei einer Vernetzung herangezogen wird. Alle für die Kopplung von Computern und Anlagen der Telefonie erforderlichen Vorgänge können in die 7 Schichten des ISO/OSI Modells eingeordnet werden. Damit ist es für den interessierten Computernutzer leichter, sich ein Bild von den einzelnen Arbeitsschritten des Datentransportes über Netze zu machen. Dieses Modell dient an vielen Stellen in der Fachliteratur zur

Beschreibung von Spezial- und Schutzfunktionen bei Netzwerkgeräten und Software.

Teil 3 - Netzwerkprotokolle und Netzwerkdienste. Es ist die Sprache der Netzwerkgeräte, die erst den eigentlichen Datentransport zwischen Computern ermöglicht. Dieser Teil befaßt sich exemplarisch mit einigen Protokollen der TCP/IP Familie, die zur Realisierung von Netzdiensten erforderlich sind. Dabei bauen höhere und komplexere Protokolle auf einfacheren Basisprotokollen auf, es gibt also eine Hierarchie von Netzwerk-Protokollen.

10:30 Uhr - Pause

11:00 Uhr - Block 3 - Grundlagen der IT-Sicherheit

Teil 1 - IT-Sicherheit, Datenschutz und Informationsschutz, was ist was? Der Datenschutz befaßt sich mit dem Schutz personenbezogener und personenbeziehbarer Daten. Das deutsche Bundes-Datenschutzgesetz BDSG gilt in diesem Bereich als weltweit führend und vorbildlich. Informationsschutz wird in Behörden und Unternehmen betrieben, um 'Staats- und Firmengeheimnisse' vor fremden Zugriff und Missbrauch zu schützen. Die IT-Sicherheit befaßt sich mit den Schutzaspekten Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und wie man sie bei Computersystemen umsetzt.

Teil 2 - Externe Systemsicherheit umfaßt Maßnahmen, die in einem Computersystem ergriffen werden, um einen möglichen Angreifer gar nicht erst in das System gelangen zu lassen. Sie ist die erste äußere Schale, die überwunden werden muß, damit auf die internen Funktionen zugegriffen werden kann. Es gilt also diese äußere Schale zu härten, um einen robusten und sicheren Computerbetrieb gewährleisten zu können.

Teil 3 - Interne Systemsicherheit beschreibt die Mechanismen, die verhindern sollen, daß ein Computerbenutzer höhere Berechtigungen auf dem System erlangen kann. Es geht also darum, daß Benutzer sich keinen ungewollten privilegierten Status in einem System erschleichen oder sich als andere Benutzer ausgeben können.

Teil 4 - Netzwerksicherheit umfaßt die Maßnahmen, die ergriffen werden, um Computer und ihre Dienste in einem Netzwerk robuster gegen Angriffe oder Missbrauch zu machen.

12:30 Uhr - Mittagessen

14:00 Uhr - Block 4 - Von Firewalls, DMZ und Verschlüsselung

Teil 1 - Schutz gegen Angriffe aus dem Internet, die Firewall und die 'demilitarisierte Zone (DMZ)'. Was ist eine Firewall und was kann sie leisten und gegen welche Art von Angriffen ist sie unwirksam? Was verbirgt sich hinter einer DMZ? Wie können diese Einrichtungen abgesichert und wie können sie auf Wirksamkeit überprüft werden?

Teil 2 - Wächterdienste, oder was ich nicht weiß, macht mich nicht heiß!!! Warum werden nicht alle Angriffe aus dem Internet verhindert oder zumindest rechtzeitig erkannt? Auf diese Frage folgt die Erkenntnis, daß Computersoftware nun einmal nicht fehlerfrei ist und man sich nur gegen die Angriffe wehren kann, die man auch bemerkt. Wie verlaufen heute gezielte Angriffe und durch welche Maßnahmen kann man sie ggf. besser erkennen? Wie funktioniert ein 'Man in the middle' oder 'Denial-of-Service (DoS) attack'? Was ist ein Fishing-Angriff?

Teil 3 - Was ist eine Public-Key-Infrastructure (PKI), wozu ist sie gut und wie funktioniert sie? Die Verwendung von Datenverschlüsselung, Signatur und starken Authentisierungsmethoden erfordert die sichere Handhabung von Computerzertifikaten. Diese 'Personalausweise' der Computerwelt müssen auf sichere Weise erzeugt, gespeichert und transportiert werden. Dafür sind einige hoch spezialisierte Dienste erforderlich.

Teil 4 - Wie funktioniert Datenverschlüsselung und welche grundsätzlichen unterschiedlichen Arten der Verschlüsselung gibt es?

15:30 Uhr - Pause

16:00 Uhr - Block 5 - Neue Medien und Big-Data, alles was schick und hipp ist

Teil 1 - Von Facebook, Twitter, DropBox und Co. Was kann man in Social-Media publizieren und was gehört definitiv nicht ins Netz? Schutz persönlicher Informationen, wie geht das im Internetzeitalter? Wenn persönliche Disziplin in Verbindung mit Verschlüsselung eingesetzt wird, ist eine Basissicherheit für die Nutzer von modernen Medien erreichbar. Dies hat jedoch Grenzen, wenn es um sensible Informationen geht.

Teil 2 - Alles geklaut, in der Cloud? Fast alle wichtigen Dienste werden heute bereits als Cloudlösungen angeboten, d. h. sie werden an einem beliebigen Ort auf der Erde in einem Rechenzentrum betrieben und der Benutzer kann über das Internet auf diese Dienste zugreifen. Dies ist für einige Services durchaus sinnvoll, hat jedoch auch in vielerlei Hinsicht seine Grenzen und

Nachteile. Insbesondere bei existenziellen Computeranwendungen muß geprüft werden, ob ein Betrieb in der Cloud verantwortbar ist oder nicht. Am Beispiel der iCloud von Apple und O365 von Microsoft werden diese Aspekte erläutert.

Teil 3 - Die Zukunft von Big-Data und zentralen IT-Services hat längst begonnen. Wo führt uns dieser Weg hin? Was kommt nach iCloud und O365?

Teil 4 - Buchtipp: „Sie kennen Dich, sie haben Dich, sie steuern Dich“ von Markus Morgenroth. Von Big-Data und seinen Gefahren für jeden einzelnen von uns!

17:30 Uhr - Abendessen

19:00 Uhr - Block 6 - Raum für Fragen und Diskussion

20:00 Uhr - Ende Tag 2

4.3 - Tag 3, Sonntag 4.10.2015

09:00 Uhr - Block 7 - Was kann ich selbst für die Sicherheit meiner Daten und Computersysteme tun?

Teil 1 - Wie verhalte ich mich sicher im Internet und welche Funktionen sollte ich besser nicht nutzen?

Teil 2 - Wie kann ich meine Daten schützen?

Teil 3 - Computer sind wie Haustiere, sie brauchen Pflege!

Teil 4 - Sind Datensicherungen wirklich nur etwas für Feiglinge?

Teil 5 - Die Zukunft, was wird sich ändern?

10:30 Uhr - Pause

11:00 Uhr - Block 8 - Raum für offene Fragen und Feedback der Seminarteilnehmer.

12:00 Uhr - Mittagessen, Seminarende

5. Seminarleitung

Dieses Wochenendseminar wurde geplant und wird geleitet von Wolfgang Werner Weyrich. Er ist blind und befaßt sich seit 1996 beruflich mit IT-Sicherheit und arbeitet als Diplom Informatiker im Bereich der IT-Sicherheit bei der ZF Friedrichshafen AG in Saarbrücken. Hier verantwortet er das Fachgebiet IT-Security Governance für die ZF Informatik weltweit.

Telefon: 06 81 / 6 62 49

E-Mail: wolfgang.weyrich@zf.com

6. Anmeldung

Anmeldungen zu diesem Seminar bitte direkt im Aura-Hotel Saulgrub:

Telefon: 0 88 45 / 9 90

E-Mail: aura-hotel@bbsb.org

Änderungen vorbehalten