42 32

Das Softwarepark Hagenberg Magazin | Ausgabe 2018

LANGE NACHT der FORSCHUNG

Eintritt frei!

13. April 2018

Erleben Sie Forschung live
im Softwarepark Hagenberg!

www.LangeNachtderForschung.at

Die VLW - Ihr Partner für Ihr Wohlfühl-Zuhause in OÖ und Ihre berufliche Zukunft in Hagenberg

- Im multifunktionalen **Arbeiten und Wohnen** stehen maßgeschneiderte Bürowelten in flexiblen Größen zur Verfügung.
  Die 28-145 m² großen Büroflächen verfügen über eine direkte Anbindung an den Softwarepark.

- Sehr zentral in der **Hauptstraße**, moderne Mietwohnungen und barrierefreie, altersgerechte Wohnungen mit 50-90 m² Wohnfläche. Großzügig geplant und nach Süden ausgerichtet bieten diese Wohnungen die optimalen Voraussetzungen für Sie und Ihre Familie.

- Bereits in Bau: Mietwohnungen in **Pregarten**
  Infos und Wohnungsbewerbung ab sofort

Infos:

Fr. Moser, Tel.: (0732) 653461-37
birgit.moser@vlw.at
www.vlw.at

VLW
Im Leben zu Hause

4232 INHALT

Sehr geehrte LeserInnen,

die Vielfalt des Softwarepark Hagenberg spiegelt sich auch in der Zusammenarbeit unserer Partner aus Forschung, Ausbildung und Wirtschaft wider und ist in unseren Strukturen tief verankert.

Dazu vorab vier kurze Stellungnahmen zum Thema Information Security:

Foto: JKU

Rektor Univ.-Prof. Mag. Dr. Meinhard Lukas
Rektor der Johannes Kepler Universität und Leiter des Softwarepark Hagenberg

Information Security – mit Sicherheit existenziell

Technologische Sicherheit ist allumfassend, das Thema Information Security existenziell. Ein Hack kann uns alle treffen und weitreichende Folgen haben. Mit seiner Expertise auf diesem Sektor setzt der Softwarepark Hagenberg nun neue Maßstäbe, die Synergieeffekte mit dem stetig wachsenden Linz Institute of Technology (LIT) sind wertvoll und nachhaltig für den gesamten Standort. Das Team aus engagierten WissenschafterInnen überzeugt einmal mehr als Triebfeder, Tempomacher und als Tonangeber.

Foto: FH OÖ

FH-Prof. DI Robert Kolmhofer
Leiter Department Sichere Informationssysteme FH OÖ

Information Security betrifft alle – besonders 2018

Fast täglich hört und liest man von IT-Security-Vorfällen und erfolgreichen Cyber-Attacken. Umso wichtiger ist es daher, das erforderliche Know-how im Bereich Informationssicherheit/IT-Security/Datenschutz für Unterehmen, Organisationen und Behörden anwendbar zu transportieren.

Der Softwarepark ist für das Information Security Jahr 2018 durch das Department Sichere Informationssysteme der FH OÖ mit seinen international anerkannten Security Studiengängen und Forschungsaktivitäten, die JKU, SCCH, Beratungsunternehmen im Information Security Bereich und viele IT-Unternehmen der ideale Ort für ein spannendes und informatives Veranstaltungsjahr.

BRÜCKENPFEILER

Editorial

Foto: SWPH

Dr. Sonja Mündl
Managerin des Softwarepark Hagenberg

Der Countdown läuft!

Mit Stichtag 25. Mai 2018 wird die DSGVO für alle innerhalb der EU bindend. D.h. viele haben ihren Datendschungel schonungslos zu lichten – und als allererstes eine Bestandaufnahme all ihrer gespeicherten Daten vorzunehmen.

Im Rahmen des heurigen Leitthemas „Information Security" widmet sich der Softwarepark Hagenberg zahlreichen Veranstaltungen, wie der spannenden Eventreihe für IT-ExpertInnen, dem Security Forum und der Langen Nacht der Forschung, welche im Softwarepark Hagenberg stattfinden (Näheres auf Seite 19).

Foto: STIWA Group

Dipl.-Ing. Thomas Führer, MSc
Obmann des Unternehmensnetzwerk Softwarepark Hagenberg

Dem Information-Security-Hype voraus

Im Softwarepark Hagenberg kooperieren mehr als 75 Unternehmen sowie Ausbildungs- und Forschungseinrichtungen zum Thema IT – mit Sicherheit. Im Jahr 2000 ist mit der Gründung des ersten Studiengangs zu Computer und Mediensicherheit die Wichtigkeit von Information Security lange vor dem aktuellen Hype in Hagenberg angekommen. Der Zugang zu AbsolventInnen stellt den Unternehmen permanent SpezialistInnen mit umfangreichem Know-how zur Verfügung. Davon profitieren sowohl der Softwarepark als auch seine Kunden.

Lassen Sie uns vernetzen!
Wir freuen uns darauf, Sie bei unseren spannenden Veranstaltungen im „Information Security Park Hagenberg" zu treffen.

JKU JOHANNES KEPLER UNIVERSITÄT LINZ

softwarepark hagenberg
business research education

Der Softwarepark Hagenberg ist Forschungs-, Ausbildungs- und Wirtschaftsstandort. Als Spin-off der Johannes Kepler Universität (JKU) Linz, gegründet von Univ.-Prof. Dr. Bruno Buchberger, trägt er bis heute wesentlich zur Innovationskraft Oberösterreichs bei. Modernste Infrastruktur, sowie ein vielfältiges Netzwerk aus erfahrenen BranchenexpertInnen, jungen Kreativen und wissbegierigen Studierenden zeichnen den Softwarepark aus. Insbesondere diese Synergie ist ein wesentlicher Teil des Erfolgskonzeptes. Denn der Softwarepark Hagenberg ist ein Ort der Kommunikation und Begegnung an dem rund 2.800 Menschen arbeiten, forschen, lehren, lernen und leben.

INFORMATION SECURITY UND DATENSCHUTZ NEU – WICHTIG FÜR WEN?

EVENTREIHE FÜR IT-EXPERT|INNEN

INFORMATION SECURITY

IM SOFTWAREPARK HAGENBERG

08.FEBRUAR | 21.JUNI | 22.NOVEMBER 2018

Anzeige, Foto: ranjith ravindran | Shutterstock.com

SICHERER ERFOLG!

Die Softwarepark Hagenberg Eventreihe.

Im Jahr 2016 formierte sich eine ExpertInnengruppe aus Vertretern der Unternehmen, Forschungsinstitute und Bildungseinrichtungen des Softwarepark Hagenberg, um die Idee einer neuen Hagenberger Eventreihe als gemeinsames Forum für Inspiration, Präsentation, Kooperation und Kommunikation nach innen und außen zu verwirklichen.

Das fünfköpfige Team, bestehend aus Dipl.-Ing. Thomas Führer, MSc (STIWA Group), DI (FH) Thomas Kern (FH OÖ Campus Hagenberg), DI Theodorich Kopetzky (Software Competence Center Hagenberg – SCCH), Dr. Sonja Mündl (Softwarepark Hagenberg) und A.Univ.Prof. Dipl.-Ing. Dr. Wolfgang Schreiner (Research Institute for Symbolic Computation (RISC) der JKU), konkretisierte diese Idee und setzte sie im Jahr 2017 im Zuge von mehreren aufeinander aufbauenden offenen Veranstaltungen um. Im Rahmen von Vorträgen eingeladener renommierter Fachleute aus Wirtschaft und Wissenschaft sollten die TeilnehmerInnen mehr über aktuelle Trends und daraus resultierende IT-Anforderungen erfahren, um in anschließender Diskussion ausgewählte Themengebiete zu vertiefen und gemeinsam Lösungsmöglichkeiten zu erörtern.

Jährlich ein hochrelevantes Leitthema

Der Konsens, pro Jahr ein übergeordnetes, für alle Beteiligten hochrelevantes Leitthema zu definieren, war schnell gefunden. So widmete sich der erste Zyklus im Jahr 2017 dem Thema „Automotive Computing“. In drei erfreulich gut besuchten Veranstaltungen wurde gemeinsam mit internationalen ExpertInnen erörtert, welche neuen Herausforderungen insbesondere die Mobilität der Zukunft an die Informationstechnologie stellt, welche zunehmend wichtige Rolle das Thema Datenanalyse im Automobilbereich spielen wird und wie den steigenden Safety- und Security-Anforderungen beim autonomen Fahren begegnet werden kann.

Gerade das Thema Informationssicherheit wurde in der Vergangenheit meist etwas stiefmütterlich behandelt. Allerdings steigt mit der massiv wachsenden Menge an informationsverarbeitenden und zunehmend vernetzten Systemen in immer komplexeren Anwendungsbereichen auch das daraus resultierende Bedrohungspotential. Nicht zuletzt schwebt auch die Europäische Datenschutzgrundverordnung, die am 25. Mai 2018 in Kraft tritt, wie ein Damoklesschwert über den Köpfen der Unternehmen.

Damoklesschwert Europäische Datenschutzverordnung

Eine umfassende Betrachtung von Sicherheitsmaßnahmen bezüglich der Aspekte Technik, Architektur und Management ist daher unerlässlich. Sie bietet allerdings auch die Chance nicht nur die Infrastruktur nach dem Stand der Technik aufzustellen, sondern auch Datenmanagement und Unternehmensprozesse besser gestalten zu können.

Aus diesem Grunde werden die Veranstaltungen im Jahr 2018 unter dem Leitthema „Information Security“ stehen. Erneut werden wir zusammen mit namhaften ExpertInnen die Materie aus unterschiedlichen Blickwinkeln beleuchten. Dazu gehören unter anderem das Internet of Things, Embedded Systems, Smart Cloud Services, Kritische Infrastrukturen, Landwirtschaft und Lebensmittel, Gesundheitswesen und Medizintechnik, sowie rechtliche Aspekte.

Aufgrund der hohen Aktualität des Themas Recht in der IT-Security, ist der Titel der Auftaktveranstaltung am 08. Februar 2018 bereits Programm: „Damoklesschwert - Schutz kritischer Infrastrukturen“

Wir hoffen, auch Sie sind von Anfang an mit dabei! Denn die Softwarepark Hagenberg Eventreihe ist mit Sicherheit ein Erfolg!

DI (FH) Thomas Kern
FH OÖ Campus Hagenberg, Leiter Center of Excellence

Foto: Nata-Lia | Shutterstock.com

Informationssicherheit im organisatorischen (Information Security Management) und technischen (IT-Security) Bereich ist aus unserer digitalisierten vernetzten Welt nicht mehr wegzudenken. Täglich erreichen uns Meldungen über Sicherheitsvorfälle, seien es „Hacks" von Internetplattformen oder Firmenservern, Schwachstellen in der Firmware von Produkten, die zu Sicherheitslücken führen oder auch Data Leaks, die durch Ausnutzung mangelnder Informationssicherheitsmaßnahmen erst ermöglicht wurden. Um Information Security sicherzustellen ist ein ganzheitlicher Ansatz im Produktlebenszyklus technisch und organisatorisch erforderlich.

Bei der Auftaktveranstaltung am 08. Februar 2018 spricht Mag. Walter Unger in seiner Keynote über das Thema „Cyber Defence - welche Fähigkeiten brauchen wir?". Der Softwarepark Hagenberg hat ihn vorab bereits zum Interview gebeten.

Mag. Walter J. Unger
Oberst des Generalstabsdienstes

Foto: BMLV/privat

„Eine Störung oder gar Zerstörung der strategischen Infrastrukturen kann schwerwiegende Auswirkungen auf das Wohl der Bevölkerung haben."

Theresianische Militärakademie 1979-1982, seit 1982 Kommandanten- und Leiterfunktionen in der Truppe sowie der Zentralstelle des BMLVS; 1988-1991 Generalstabsausbildung; 1998-1999 Führungskräftelehrgang des Bundes, 1999-2000 Kommandant des Panzerabwehrbataillons 1; 2001-2009 Leiter Elektronische Abwehr, 2006-2008 Leiter der Interministeriellen Arbeitsgruppe Strategie „IKT-Sicherheit", 2009 Leiter der Abteilung IKT-Sicherheit, seit Mai 2013 Leiter der Abteilung Cyber Defence & IKT-Sicherheit im Abwehramt, derzeit Leiter Cyber-Verteidigungszentrum (Cyber Defence Centre).

Was sind Betreiber wesentlicher Dienste (BwD) bzw. Betreiber kritischer Infrastrukturen und welche Bedeutung haben diese für den Staat (Gesellschaft, Wirtschaft, Regierung, Exekutive, Landesverteidigung)?
Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit (lebens-) wichtiger strategischer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Störung für größere Bevölkerungsgruppen nachhaltig wirkende Versorgungsengpässe oder andere dramatische Folgen eintreten. Staat und Gesellschaft funktionieren nur dann, wenn Infrastrukturen wie z. B. Telekommunikation, Energieversorgung (Elektrizität, Öl, Gas), Bank-, Finanz-, und Verkehrswesen, Gesundheitswesen (einschließlich Lebensmittel- und Trinkwasserversorgung und Entsorgung), Notfall und Rettungsdienste, Regierung und öffentliche Verwaltung (einschließlich Polizei, Zoll und Bundesheer) ohne wesentliche Beeinträchtigung verfügbar sind. Diese Infrastrukturen sind das Rückgrat einer erfolgreichen Wirtschaft, einer lebendigen Forschungsgemeinschaft, eines transparenten Staates sowie einer freien Gesellschaft.

Warum ist ein Schutz dieser kritischen Infrastrukturen in den Bereichen Netzwerk- und Informationssicherheit so wichtig?
Schon immer waren Staaten von ihren strategischen Infrastrukturen abhängig. Die Digitalisierung und Vernetzung der strategischen Infrastrukturen und aller Gesellschaftsbereiche führt zu einer massiven Abhängigkeit von der Verfügbarkeit, Vertraulichkeit und Integrität der gespeicherten Daten, der Funktionsfähigkeit der IKT-Infrastrukturen und dem reibungslosen Fluss riesiger Datenmengen über komplexe Netze. Eine Störung oder gar Zerstörung dieser Infrastrukturen kann schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von staatlichen Einrichtungen haben.

In der Öffentlichkeit wird oft vom „Cyber Security Gesetz" gesprochen, das dafür 2018 in Österreich in Kraft treten soll. Warum ist Cyber Security für die BwD von essentieller Bedeutung?
Der Wirtschaftsstandort, die Daseinsvorsorge, Gesellschaft und Staat sind vom Funktionieren der strategischen Infrastrukturen und der Informations- und Kommunikationsflüsse abhängig. Der Schutz dieser Infrastrukturen hat daher strategische Bedeutung! Nicht nur für den Staat, sondern auch für sehr viele Unternehmen!

Gibt es öffentlich bekannte Beispiele für Cyber-Angriffe auf Betreiber wesentlicher Dienste?
In den letzten beiden Jahren gibt es international und in Österreich zahlreiche Beispiele für derartige Angriffe. Ende 2016 legten Cyber-Angriffe die Stromversorgung in der Ukraine lahm. Hundertausende waren für bis zu 48 Stunden ohne Strom. Der Versuch ein Bot-Netz aufzubauen, legte ca. 900.000 Router der deutschen Telekom lahm. Im Mai 2017 verursachte die Erpressersoftware NonPETYA bei der Fa. Maersk, einer der weltgrößten Logistikunternehmen, binnen Minuten einen Schaden von mehreren Hundert Millionen. Im Februar 2016 wurde die Telekom

CYBER DEFENCE

Ein Interview mit Mag. Walter J. Unger, Oberst des Generalstabsdienstes, Leiter der Abteilung Cyber Defence & IKT-Sicherheit im Abwehramt des BMLVS.

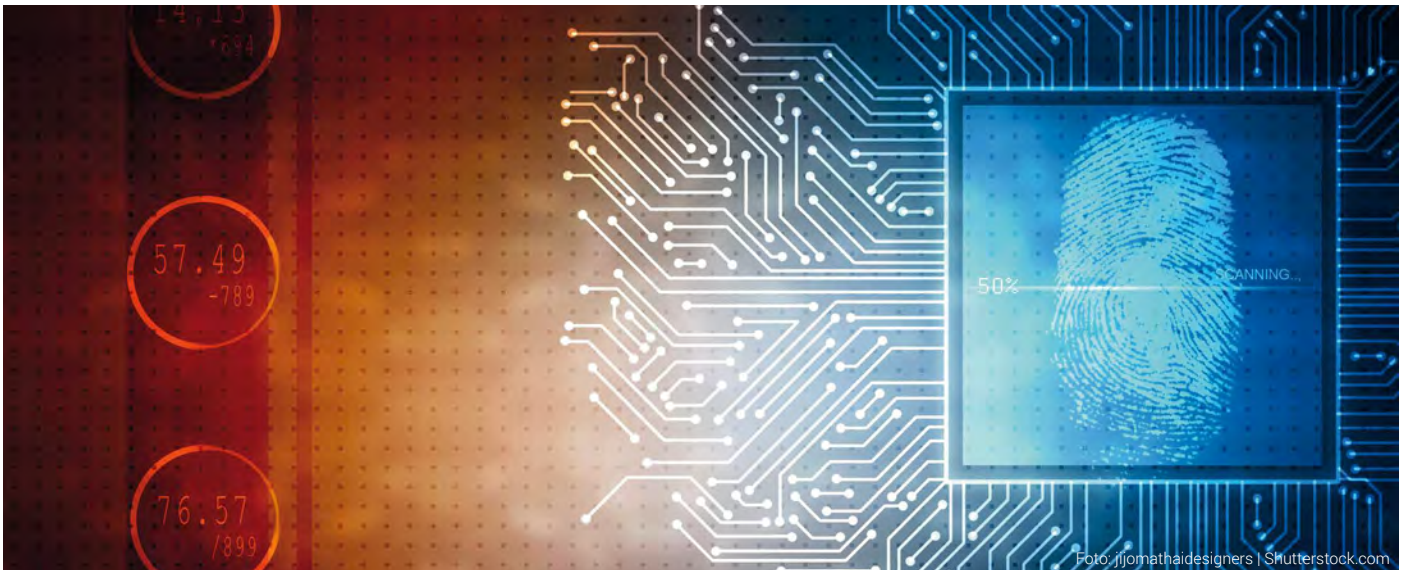

Foto: jijomathaidesigners | Shutterstock.com

Austria Ziel eines DDoS-Angriffes, was dazu führte, dass die mobilen Datendienste über mehrere Stunden für eine große Zahl der Kunden nicht verfügbar waren. Zwischen September 2016 und Dezember 2017 gab es zahlreiche politisch motivierte DDoS-Angriffe auf Webseiten österreichischer Institutionen (darunter der Flughafen Wien, das Außenministerium, das Landesverteidigungsministerium, die Nationalbank, das Parlament, die Seite des damals noch Präsidentschaftskandidaten Van der Bellen, die Seite einer politischen Partei etc.).

Auch das Österreichische Bundesheer (ÖBH) ist permanent Angriffen ausgesetzt. Pro Tag werden im Durchschnitt etwa 60.000 Events registriert. Nach entsprechenden Analysen verbleibt ca. 1 konkreter Angriff pro Tag. Vielfach handelt es sich um breit gestreute Massenangriffe, einige gezielte Angriffe weisen jedoch die Merkmale von international angesetzten Cyber-Spionagekampagnen auf.

Was können die Auswirkungen von Cyber-Angriffen für die Öffentlichkeit sein?
Schäden für Einzelpersonen enstehen vor allem durch den Missbrauch personenbezogener Daten, Cyber-Mobbing und durch Cyber-Kriminalität. Unternehmen, Behörden usw. müssen vor allem mit Erpressung mittels Verschlüsselungstrojaner oder DDoS-Attacken rechnen. Das Know-how, Firmen und Betriebsgeheimnisse sind durch Cyber-Spionage bedroht. Sabotage-Angriffe können zu großen finanziellen Schäden führen und Reputationsverlust droht, wenn Kundendaten gestohlen werden. Angriffe gegen einzelne kritische Infrastrukturen könnten z.B. ein Blackout verursachen. Auch großangelegte Angriffe auf die Souveränität Österreichs sind vorstellbar. Deswegen ist das BMLVS beauftragt worden, die Landesverteidigung auch im Cyber-Raum vorzubereiten.

Gibt es schon eine Orientierungsmöglichkeit, wer in Österreich als BwD eingestuft werden wird, bzw. woran kann man sich orientieren, ob man als BwD betroffen sein könnte?
In Österreich werden ca. 400 Unternehmen zur kritischen Infrastruktur gezählt. Das Bundeskanzleramt analysiert derzeit, welche Unternehmen als BwD einzustufen sind. Spätestens im Herbst 2018 muss diese Liste fertig sein und die Unternehmen werden schriftlich informiert.

Inwieweit sind auch Zulieferer oder Dienstleister von BwD von der EU NIS-RL mit umfasst?
Wenn man über Cyber-Sicherheit nachdenkt, dann wird schnell klar, dass der ganze Lebenszyklus eines wichtigen IKT-Systems betrachtet werden muss. Ein ganzheitlicher, systemischer Ansatz umfasst schließlich personelle, organisatorische, infrastrukturelle und technische Absicherungsmaßnahmen. Es ist daher logisch, dass Zulieferer, Dienstleister, Partner und Kunden beim Sicherheitskonzept berücksichtigt werden müssen.

Welche Schutzmaßnahmen sollen BwD ab Mai 2018 treffen?
Die Betreiber haben geeignete organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Netz- und Informationssysteme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Dienste maßgeblich sind. Dabei ist der Stand der Technik einzuhalten. Das NIS-Gesetz sieht vor, dass Sicherheitsstandards auf dem aktuellen Stand der Technik vorgegeben werden. Diese Standards werden derzeit von einer Arbeitsgruppe beim Bundeskanzleramt erarbeitet. >>

CYBER DEFENCE

Fortsetzung des Interviews mit Mag. Walter J. Unger.

Wer wird in Österreich die von BwD getroffenen Maßnahmen überwachen?
Die Betreiber haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Abs. 1 auf geeignete Weise gegenüber dem Bundesminister für Inneres nachzuweisen. Der Bundesminister für Inneres kann zur Kontrolle der Einhaltung der Anforderungen Einschau in die Netz- und Informationssysteme und Unterlagen nehmen und ist ermächtigt, Maßnahmen zur Herstellung der Sicherheitsanforderungen zu verlangen.
Gemäß Entwurf NIS-Gesetz werden dafür drei NIS-Behörden eingerichtet: eine beim Bundeskanzler, eine beim Innenminister und eine beim Verteidigungsminister.

Welche Rolle wird das BMLV im Bereich BwD spielen?
Das BMLV ist NIS-Behörde für alle militärischen Angelegenheiten. Ob das BMLV auch eine Zuständigkeit für jene BwD, die für die Aufgabe Landesverteidigung von besonderer Bedeutung sind, erhält, ist noch nicht entschieden.

Welche Maßnahmen hat ein BwD im Falle eines Cyber-Angriffs mit Auswirkungen auf seine betriebene kritische Infrastruktur zu setzen?
Nebst den präventiven Maßnahmen zum Eigenschutz und der Abwehr der laufenden Angriffe, haben die BwD einen Sicherheitsvorfall unverzüglich an das für sie zuständige Computer-Notfallteam zu melden, welches die Meldung unverzüglich an den Bundesminister für Inneres weiterleitet.

Natürlich wird eine neue Richtlinie/Gesetz nur dann ernst genommen, wenn es bei Verstößen auch Strafen gibt. Mit welchen Strafen hat ein BwD zu rechnen, wenn die in der EU NIS-RL geforderten Maßnahmen nicht umgesetzt werden?
Mit Geldstrafen bis zu 50.000,- Euro, im Wiederholungsfall bis zu 100.000,- Euro muss rechnen, wer den Verpflichtungen zur Mitwirkung, zur Auskunftserteilung, zur Nachweiserbringung bzw. wer die Einschau oder die Umsetzung der Empfehlungen verweigert oder der Meldepflicht bei Sicherheitsvorfällen nicht nachkommt.

SICHERES NETZWERK

TeleTrusT - Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa.

TeleTrusT bietet Foren für ExpertInnen, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der „TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate „TeleTrusT Information Security Professional" (T.I.S.P.) und „TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens „IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

In enger Zusammenarbeit mit der Bundesgeschäftsstelle des Verbandes in Berlin hat die FH Oberösterreich Campus Hagenberg als „TeleTrusT-Regionalstelle Hagenberg" die TeleTrusT-Repräsentanz vor Ort übernommen.

www.teletrust.de

TeleTrusT
Pioneers in IT security.

DER FAKTOR MENSCH

Wichtiger Bestandteil der Informationssicherheit bei vernetzter Produktion.

Information Security ist nicht zuletzt aufgrund aktueller Vorfälle in den Medien allgegenwärtig. Die STIWA Group investiert seit Jahrzehnten vermehrt in das Thema Informationssicherheit und nutzt dabei die Kompetenzen aus dem Softwarepark Hagenberg.

Die STIWA Group ist im Softwarepark Hagenberg mit ihren Geschäftsbereichen Manufacturing Software, Laborautomation und Gebäudeautomation ansässig. Gerade in diesen Bereichen ist das Thema Informationssicherheit von besonderer Relevanz für die STIWA Group, da mit den Softwarelösungen der Unternehmensgruppe hochsensible Produktions-, Anlagen- oder Patientendaten verarbeitet werden – und das weltweit.

Bewusstsein schaffen

Eine global vernetzte Produktion, bei der unter anderem vollautomatisiertes Datenmanagement und Maschine-zu-Maschine-Kommunikation notwendig sind, bedingt die Verarbeitung großer Datenmengen. Diese Daten können vertrauliche Informationen enthalten, etwa über Produktionsprozesse, Teilequalität und MitarbeiterInnen. Nicht nur grundlegende Aspekte wie Netzwerksicherheit müssen dabei beherrscht werden: die MitarbeiterInnen müssen darüber hinaus ein Bewusstsein gegenüber Praktiken wie Social Engineering oder Phishing entwickeln. Die STIWA Group kennt diese Materie nicht nur aus Sicht des Softwareentwicklers für die Fertigungsautomation, sondern auch aus der Sicht des Anlagenbauers und des Kunden: Am Stammsitz in Attnang-Puchheim fertigt das Unternehmen Hochleistungs-Montageanlagen, in Gampern setzt die STIWA Group ihre Produktionsanlagen und -software zur Herstellung von Teilen und Komponenten für die Automotive-Industrie ein. Aus dieser umfassenden Sicht auf das Thema entwickelte sich auch der ganzheitliche Ansatz bei Informationssicherheit im Unternehmen: „Der Faktor Mensch muss bei der Evaluierung der Sicherheitsrisiken im produzierenden Umfeld ebenso in Betracht gezogen werden wie Sicherheitslücken in technischen Systemen“, sagt Alexander Schwarz, Information Security Manager bei STIWA.

Umfassende Maßnahmen

Um ein möglichst gutes Schutzniveau der Daten gewährleisten zu können setzt die STIWA Group auf intensive Aus- und Weiterbildungsmaßnahmen. Dazu entwickelte das Unternehmen ein eigenes Security Awareness Programm, in dem durch regelmäßige Schulungen zum Thema das Bewusstsein gegenüber möglichen Angriffen erhöht wird. Zusätzlich unterstützt ein Sicherheitsleitfaden die MitarbeiterInnen bei der täglichen Arbeit. Regelmäßige Newsletter warnen vor aktuellen Angriffswellen und erhöhen die Aufmerksamkeit der Belegschaft gegenüber konkreten Themen punktuell. Bestehen aktuelle Bedrohungen, werden dabei auch spezielle Maßnahmen kommuniziert. Eine eigens eingeführte Kolumne für Information Security in der MitarbeiterInnenzeitung, in der aktuelle Themen aus dem Bereich Informationssicherheit von ExpertInnen diskutiert werden, ist ebenso Teil des aktuellen Security Awareness Programms.

www.stiwa.com

Foto: HYWARDS | istock.com

Entgeltlicher Beitrag

DISCONSULTING

Datenschutz und Informationssicherheit.

Die EU Datenschutzgrundverordnung trifft jedes Unternehmen

Die neue EU Datenschutzgrundverordnung (DSGVO) ist am 24. Mai 2016 in Kraft getreten und wird am 25. Mai 2018 durch das neue österreichische Datenschutzgesetz in Geltung erwachsen. Es wird damit auch in Österreich das einheitliche Unionsrecht zum Schutz von personenbezogenen und sensiblen Daten umgesetzt. Mit der DSGVO werden insbesondere Datenschutzmaßnahmen für die Verarbeitung von personenbezogenen Daten im organisatorischen und technischen Bereich nach dem Stand der Technik, Meldepflichten, regelmäßige Audits und Wirksamkeitsprüfungen vorgeschrieben. Anstelle der DVR-Meldung muss der Verantwortliche selbst für ein Verzeichnis der DSGVO-relevanten Anwendungen sorgen und unter gewissen Rahmenbedingungen einen Datenschutzbeauftragten nominieren. Bei Verstößen gegen die DSGVO drohen hohe Strafen von bis zu mehreren Mio. EUR, unabhängig von der Unternehmensgröße. Eine rechtzeitige, professionelle Umsetzung der DSGVO-Auflagen ist daher unumgänglich.

Beratungskompetenz durch kompetente Partner

UNINET unterstützt in Kooperation mit der auf Datenschutz- und Informationssicherheitsrecht spezialisierten Rechtsanwaltskanzlei Prof. Hintermayr und Partner österreichische Unternehmen mit dem Beratungsprodukt „DISconsulting – Datenschutz und Informationssicherheit“ bei der zielgerichteten Analyse, um die Verpflichtungen der Unternehmen in Bezug auf die Anforderungen der DSGVO zu identifizieren und die erforderlichen Umsetzungsmaßnahmen zum Schutz der personenbezogenen Daten und Anwendungen realisieren zu können. Der Informationssicherheits-/IT-Security-Part wird dabei von den ExpertInnen der UNINET wahrgenommen, die über langjährige Erfahrung im Bereich IKT/IT-Security/-Informationssicherheitsconsulting in einer Vielzahl von Projekten für KMUs und Großkonzerne bis hin zu multinationalen Unternehmen verfügen. Der datenschutz-/informationssicherheitsrechtliche Teil der Beratungsdienstleistung wird von der Rechtsanwaltskanzlei Prof. Hintermayr & Partner, durch den IT-Rechtsexperten FH-Prof. Mag. Dr. Peter Burgstaller, LL.M. durchgeführt. Diese Bündelung von technischer und rechtlicher Expertise erlaubt somit eine umfassende Abdeckung aller relevanten Belange mit Bezug auf die Anforderungen aus der DSGVO.

Datenschutz- und Informationssicherheits-Assessment

Die Kernbereiche von DISconsulting sind dabei, die Erhebung, welche personenbezogenen Daten in welchen Anwendungen verarbeitet werden, die Analyse und Abschätzung der Risiken im Rahmen der Verarbeitung, die Analyse bestehender Informationssicherheitsmaßnahmen und welche zusätzlichen technischen und organisatorischen Maßnahmen (datenschutzfreundliche Voreinstellungen, Sicherheit der Verarbeitung) umzusetzen sind. Darüber hinaus werden die rechtlich erforderlichen Maßnahmen, wie die Führung eines Verarbeitungsverzeichnisses oder auch die Informations- und Meldepflichten bei Datenschutzvorfällen, definiert.

www.uninet.at

ENG VERNETZT

Das Security Forum für ExpertInnen der Informationssicherheit.


Foto: jijomathaidesigners | Shutterstock.com

Der Hagenberger Kreis (HK) ist ein Verein der Studierenden des Departments Sichere Informationssysteme der Fachhochschule Oberösterreich am Standort Hagenberg mit derzeit ca. 550 Mitgliedern. Der Verein hat es sich zum Ziel gesetzt, das öffentliche Bewusstsein für Informationssicherheit zu verbessern und untereinander auch nach dem Abschluss des Studiums in Verbindung zu bleiben.

Eines der wichtigsten Events für den HK ist das Security Forum, bei dem über die verschiedensten Aspekte der Informationssicherheit gesprochen wird. SicherheitsexpertInnen aus aller Welt treffen sich und stellen aktuelle Sicherheitsthemen vor. Die Veranstaltung findet jährlich an zwei Tagen in den Räumlichkeiten der Fachhochschule in Hagenberg statt. Die rund 200 Besucher kommen großteils aus Österreich, Deutschland und der Schweiz. Organisiert wird die Veranstaltung ausschließlich von StudentInnen – diese sind sehr stolz, dass das Security Forum am 2. und 3. Mai 2018 bereits zum 16. Mal stattfindet.

Die Veranstaltung ist für InteressentInnen mit und ohne Sicherheits-Know-How gedacht. Sowohl AdministratorInnen als auch GeschäftsführerInnen von Klein- und Mittelunternehmen sollen sich den alltäglichen Gefahren der IT-Welt bewusst werden und Wissen erwerben, wie diese Gefahren eliminiert oder umgangen werden können.

Das Security Forum besteht aus zwei parallel verlaufenden Vortagsreihen, die eine technik- und eine managementorientierte Ausrichtung haben. Jedes Jahr zeichnet sich das Security Forum durch namhafte Vortragende aus der ganzen Welt aus, die als ExpertInnen ihres Fachbereiches eine Vielfalt an Aspekten der Informationssicherheit vorstellen. Diese zeigen immer wieder auf, welche Auswirkungen der Themenkomplex „Informationssicherheit" auf die digitale Welt hat. Selbst die etwas „exotischeren" Komponenten wie Gebäudeautomatisierung, Autos, Smart Homes und industrielle Netzwerke sind davon betroffen. Vor 10 Jahren spielte Informationssicherheit in diesen Bereichen noch keine Rolle, aber seit Stuxnet hat die Forschung im Bereich industrielle Sicherheit an Fahrt aufgenommen.

Treffpunkt für SicherheitsexpertInnen

Früher war Informationssicherheit eine mystische „Black-Box", heute ist sie weit bekannt und Schwachstellen können mit einem Mausklick ausgenutzt werden. Tools, um Industrieanlagen zu hacken, sind heute frei verfügbar. Auch die Art, wie diese Systeme verbunden sind, hat sich geändert. Sie sind nicht länger abgeschottet und auch ihre proprietäre Arbeitsweise bietet keinen Schutz. Heute im Zeitalter des „Internets of Things" (IoT) und der „Industrie 4.0" müssen Systeme miteinander interagieren können. Diese Systeme sind untereinander eng vernetzt und müssen von überall erreichbar sein. Gleichzeitig muss ihre Sicherheit garantiert werden. Diese beiden Anforderungen stehen sich gegenüber und werden den HK auch in den nächsten Jahren viel beschäftigen.

www.securityforum.at

FH OÖ ALS PIONIER

Security Studiengänge seit dem Jahr 2000.

Als Trendsetter im Themenbereich Sichere Informationssysteme startete die FH OÖ Campus Hagenberg schon im Jahr 2000 mit Information Security in Forschung und Ausbildung. Heute ist das Department „Sichere Informationssysteme“ mit aktuell 9 hauptberuflichen ProfessorInnen und mittlerweile 600 AbsolventInnen eines der führenden Information Security Kompetenzzentren in Europa.

Auf den Top-Plätzen der Hochschulrankings

Aktuell werden zwei technische Studiengänge im Themenfeld Informationssicherheit und IT-Security am FH OÖ Campus Hagenberg angeboten: Sichere Informationssysteme Bachelor (SIB) und Master (SIM) sowie ein berufsbegleitender internationaler Master-Studiengang Information Security Management (ISM), der eine fundierte Ausbildung im Bereich Informationssicherheitsmanagement/Datenschutz für angehende CISOs und Datenschutzbeauftragte bietet. Über 170 aktive Studierende werden von 9 hauptberuflichen ProfessorInnen in den Bereichen Informationssicherheit & IT-Security die Schwerpunkte Netzwerktechnik und Netzwerksicherheit, Kryptographie, System- und Einsatzplanung, Secure Systems Operations, Malware, Sicheren Softwareentwurf, Informationssicherheitsmanagement, Big-Data und Cloud-Security, Forensik/Incident Analyse, Authentisierungslösungen/Smart Cards/PKI, Sichere Unternehmensorganisation/Geschäftsprozesse sowie Legal/Compliance und über 50 LektorInnen aus der Wirtschaft zu ExpertInnen, sowohl in IT-Security (mit Schwerpunkten technische Planung, Umsetzung, Betrieb und QS), als auch des Informationssicherheitsmanagements (mit Schwerpunkten ISMS, BCM, CIP, Legal/Compliance) ausgebildet. Der 6-semestrige Sichere Informationssysteme Bachelor (SIB, 180 ECTS) bietet eine fundierte Ausbildung zum technischen IT-Security Professional, der 4-semestrige Sichere Informationssysteme Master (SIM, 120 ECTS) vertieft die Ausbildung zur Expertin bzw. zum Experten für Informationssicherheit mit Forschungs-Background. Der berufsbegleitende Information Security Management Master (ISM, 120 ECTS) bietet eine berufsbegleitende Ausbildung zum CISO/CSO/DSB mit nur 8 Präsenzwochen in 2 Jahren und verwendet innovative Lehr- und Lernmethoden, wie E-Learning mit Inverted-Classroom-Konzepten. Das Department mit seinen Studiengängen ist seit Jahren in diversen Hochschulrankings auf Top-Plätzen vertreten, im FH-Ranking 2017 des Industriemagazins erreichte der Information Security Management Master als Neueinstieg sofort Platz 1 unter allen Österreichischen IT-Management-Studienrichtungen. In der dem Department Sichere Informationssysteme angeschlossenen Research-Group werden mit derzeit 8 F&E MitarbeiterInnen laufend Forschungs- & Entwicklungsprojekte in enger Verzahnung mit dem Ausbildungsbetrieb in den LABs des SIM-Masters für in- und ausländische Partner (Industrie, Behörden, Organisationen, Unternehmen) durchgeführt. Ein aktuelles Highlight im F&E Bereich ist ein Projekt in Kooperation mit dem Bundeskanzleramt/Städtebund/Gemeindebund, wo ein Maßnahmenhandbuch zur Umsetzung der Informationssicherheitsvorgaben aus der EU Datenschutzgrundverordnung für alle 2100 österreichischen Gemeinden entwickelt wird. Ein anderes aktuelles F&E Highlight ist ein Projekt mit dem Halbleitersensor-Hersteller ams (Graz/Unterpremstetten), bei dem IT-Security-Schutzmechanismen zur Kopplung von Sensor-Chips und Signalverarbeitungssoftware entwickelt werden. Mit Projekten im Sicherheitsforschungsbereich hat das Department Sichere Informationssysteme der FH OÖ Campus Hagenberg langjährige Erfahrung, unter anderem in zwei großen FFG KIRAS Projekten (Cuteforce und Realtime Analyzer) aufgebaut. Mit einem F&E Akquisevolumen von ca. EUR 0,6 Mio. pro Jahr trägt das Department maßgeblich dazu bei, dass die FH OÖ österreichweit als forschungsstärkste FH seit Jahren einen Spitzenplatz belegt.

Langjährige Erfahrung mit Projekten im Sicherheitsforschungsbereich

Das Department Sichere Informationssysteme bietet als TeleTrusT Regionalstelle Hagenberg auch internationale Vernetzung im Rahmen des größten IT-Security-Branchenverbands Deutschlands, der seinen Sitz in Berlin hat und das Who is Who der IT-Security-Industrie vereint. Die TeleTrusT Regionalstelle Hagenberg arbeitet als österreichische Drehscheibe zwischen den regionalen Mitgliedern und dem internationalen Verband, organisiert regelmäßige Beteiligungen von TeleTrusT bei Veranstaltungen wie dem Security Forum und der IKT-Sicherheitskonferenz.
Als jährliches Highlight wird vom Studentenverein des Departments Sichere Informationssysteme, dem „Hagenberger Kreis zur Förderung der digitalen Sicherheit“ (HK), das Security Forum veranstaltet, welches mit seinen über 200 (inter)nationalen BesucherInnen eine der ältesten IT-Security-Konferenzen im deutschsprachigen Raum ist. Heuer findet das Security Forum am 2./3. Mai 2018 am Campus der FH OÖ in Hagenberg bereits zum 16. Mal statt.

Alle Informationen zum Department Sichere Informationssysteme finden sich auf **www.fh-ooe.at/si**.

Entgeltlicher Beitrag

IT & MEDIEN

Studieren in Hagenberg.

20 Bachelor- und Master-Studiengänge für eine Karriere in den Bereichen Informatik, Kommunikation und Medien stehen am Campus Hagenberg der FH Oberösterreich zur Auswahl: von Software Engineering über Mediendesign, Mobile Computing und Sichere Informationssysteme bis hin zu – ganz neu – Automotive Computing und Data Science.

Praxis wird großgeschrieben

Wertvolle Praxiserfahrung sammeln die Studierenden in Projekten mit Partnern aus der Wirtschaft und im Berufspraktikum. Für ein Auslandssemester stehen rund 100 Partnerhochschulen weltweit zur Auswahl.

Studieren, forschen & arbeiten

Neben der top ausgestatteten FH sind im Softwarepark über 75 Unternehmen und zehn Forschungsinstitute beheimatet. Dies kommt auch den Studierenden zugute – in Form von Know-how-Transfer, Projekten und Praktikums- bzw. Arbeitsplätzen.

Top Karrierechancen

Neben regelmäßigen Bestnoten in Rankings zeigt auch die FH>>next Karrieremesse mit über 135 Ausstellern, wie gefragt Hagenbergs AbsolventInnen sind. Zu letzten zählen übrigens auch erfolgreiche Unternehmensgründer wie die Geschäftsführer von Runtastic, Tractive, Loxone oder Celum.

www.fh-ooe.at/campus-hagenberg

Foto: Land OÖ

Dr. Michael Strugl
Wirtschaftsreferent LH-Stellvertreter

„Die wichtigste Aufgabe ist, Anbieter und Interessenten – vor allem kleine und mittlere Unternehmen – im Bereich Informationssicherheit und Datenschutz miteinander zu vernetzen. Damit wird auch die internationale Sichtbarkeit Oberösterreichs erhöht und die regionale IT-Security-Industrie gestärkt."

Entgeltlicher Beitrag

SECURE SOFTWARE

Analytics und Informationssicherheit.

Fast jede moderne Technologie, die wir nutzen, wird von IT unterstützt. Es ist Realität, dass fast alle neuen Geräte und Maschinen IP-basiert sind. Sie bieten damit einen Port zum Internet, inklusive dem Gefahrenpotential für Cyberattacken. Dies gilt vermehrt auch für große industrielle Produktionssysteme, die noch bis vor kurzem komplett vom Internet isoliert waren. Die Erfüllung rigoroser IT-Sicherheitsanforderungen ist die Grundlage für die erfolgreiche Verwirklichung von Industrie 4.0 mit der Vision einer nahtlosen Integration ganzer Wertschöpfungsketten.

Das Software Competence Center Hagenberg (SCCH) hat sich in enger Zusammenarbeit mit der JKU als österreichisches COMET–Exzellenzzentrum (Competence Center for Excellent Technologies) national und international etabliert. Die Forschungsarbeiten des SCCH mit seinen zwei Kernkompetenzen Data Science und Software Science liefern wichtige Impulse für Informationssicherheit. Das SCCH verdankt seinen Erfolg vor allem der engen Verknüpfung der Expertisen auf diesen beiden Standbeinen und der fruchtbaren Forschungskooperation mit der JKU.

Für die nächsten 5 Jahre hat sich das Team der SCCH-WissenschaftlerInnen entschieden, ein Forschungsthema auf dem Gebiet der Informationssicherheit anzugehen, wo diese beiden Forschungskernkompetenzen perfekt eingebracht werden können, nämlich „Secure Software Analytics" (SSA). Es wird nicht zuletzt dadurch vorangetrieben, dass das SCCH hier seine jüngsten Forschungsergebnisse und Methoden aus dem Bereich Data Analytics (gemeinsam mit Instituten der JKU wie dem FAW) sehr gewinnbringend für abzeichnende IT-Security Problemstellungen nutzen können wird. Die Ergebnisse der SSA-Forschung werden für fast alle Softwarelösungen der Zukunft relevant sein, unter anderem auch Datenschutz und -sicherheit, beim verteilten Machine Learning in Cloudumgebungen.

Softwarelösungen für die Zukunft

Informationssicherheit ist auch ein Thema am FAW (JKU Linz - Institut für Anwendungsorientierte Wissensverarbeitung). Es beschäftigt sich unter anderem mit Zugriffsschutz und Anonymität von Informationen, dem Spagat zwischen Privatheit und allgemeiner Auswertbarkeit von Daten.

Die zu erwartenden Ergebnisse der Arbeiten auf dem Gebiet der Secure Software Analytics sollen in den nächsten 5 Jahren zu neuartigen Methoden und Werkzeugen für ein sicheres und nachhaltiges Software-Engineering führen, die über den Stand der heutigen Technik hinausgehen. Es zielt holistisch auf alle Schritte des Transformationsprozesses von der Spezifikation bis zum sicheren Code unter Einbeziehung einer umfassenden Analyse der Laufzeitüberwachung.

Diese in enger Zusammenarbeit mit der Industrie geplante kooperative Forschung ist auf den Bedarf der Wirtschaft abgezielt, wo idealer Weise eine Erhöhung der Produktivität in der Softwareentwicklung Hand in Hand mit einer rigorosen Einbeziehung von (Software-) Sicherheitsanforderungen erreicht werden sollte.

www.scch.at
www.faw.at

Prof. Dr. A Min Tjoa
Software Competence Center Hagenberg GmbH (SCCH), Chief Scientific Officer

Foto: SCCH

„Secure Software Analytics ist die unabdingbare Vorsorge zur Gewährleistung eines intakten Immunsystems für die Informationssicherheit."

a.Univ.-Prof. Dr. Josef Küng
Institut für Anwendungsorientierte Wissensverarbeitung (FAW), Johannes Kepler Universität Linz, Head

Foto: Privat

„Autorisierung und Zugriffskontrolle sind zentrale Bestandteile der Informationssicherheit."

ANPFIFF ZUM ANGRIFF

Limes Security spielt Ihre Verteidigung in einem Penetration Test aus. Peter Panholzer im Interview.


Foto: Limes Security GmbH

Warum glauben Sie, dass man Fußball und Penetration Tests vergleichen kann?
Wie beim Fußball wird auch bei Penetration Tests die meiste Zeit mit Training und Taktik verbracht und nicht auf dem Spielfeld. Denn im Gegensatz zu anderen schießen wir nicht einfach darauf los, sondern stecken viel Energie in die Vorbereitung.

Wie unterscheidet sich diese Vorbereitung von anderen?
In einem Kick-Off Gespräch mit dem Kunden legen wir Ziele und Nicht-Ziele fest. Damit können wir uns auf die relevanten Informationen konzentrieren und unser individuelles Vorgehen an die zu testenden Systeme anpassen. Taktisch wichtig ist für uns auch die Durchführung einer Risikoanalyse mit dem jeweiligen Unternehmen.

Wieso ist diese Risikoanalyse so wichtig?
Es ist in der Regel nicht ausreichend, nur technische Fehler zu identifizieren. Man muss auch seine architekturalen und prozeduralen Schwächen kennen. Deshalb ist zuallererst das Verständnis des gesamten Systems mit allen seinen Datenflüssen und Schnittstellen wichtig. Anschließend überlegen wir, welche Dinge passieren können und was die Auswirkungen wären. Basierend auf den Daten zeigt man schließlich konkrete Angriffswege und Bedrohungen auf. Falls es bereits Gegenmaßnahmen gibt, sollte man diese natürlich einbringen.

Wie Fußballer verbringen Sie viel Zeit mit Training und Taktik, wie hilft Ihnen das beim Test selbst?
Durch das gewonnene Wissen aus der Risikoanalyse können wir gezielt und effizient auf Schwachstellen testen, orientieren uns aber zusätzlich an Normen, wie der ISO 27000 oder der IEC 62443. Beim Test selbst setzen wir auf anerkannte Prüfwerkzeuge und implementieren bei Bedarf auch eigene. Damit die Systembetreuer schnell auf Ergebnisse reagieren können, halten wir auch ständig Rücksprache mit diesen. Unser Team ist durch umfangreiche Erfahrungen im Industriebereich jedoch hervorragend auf Tests an kritischen Systemen und Anlagen vorbereitet.

Ein Penetration Test ist also wie ein Fußballspiel, wo Sie in kurzer Zeit Spitzenleistung liefern, um Lücken in der Verteidigung zu identifizieren?
Exakt. Die gefundenen Lücken werden von uns mittels CVSS bewertet, um eine Priorisierung der identifizierten Angriffswege vorzunehmen. Anschließend empfehlen wir wirtschaftlich sinnvolle Gegenmaßnahmen. Die Ergebnisse werden als Bericht aufbereitet, der sowohl eine Management-Zusammenfassung als auch eine detaillierte Beschreibung für die Techniker enthält. Dies gibt unserem Kunden die Möglichkeit, die gefundenen Schwachstellen selbst oder mithilfe unserer ExpertInnen zu beheben.

Ist nach der Analyse dann alles abgeschlossen?
Nein. Das Wiederholen von Penetration Tests ist natürlich wichtig, um stets aktuell zu bleiben. Außerdem helfen regelmäßige Trainings das Sicherheitslevel im Unternehmen zu erhöhen.

www.limessecurity.com


Foto: Limes Security GmbH

Peter Panholzer, MSc
Geschäftsführer, Limes Security GmbH

„Im Gegensatz zu Fußball ist Security ein Spiel ohne Regeln."

IN ALLER MUNDE

Am 25. Mai 2018 tritt die EU-Datenschutzgrundverordnung in Kraft.

Das erste Datenschutzgesetz trat 1980 in Österreich in Kraft. Der Datenschutz ist damit eine relativ junge Gesetzesmaterie. In den unternehmerischen Köpfen sowie medial genoss er bisher überschaubar viel Aufmerksamkeit. Ab dem 25. Mai 2018 wird sich dies ändern, dann treten deutlich striktere Regeln und Pflichten in Kraft.

Der technologische Fortschritt, der manchmal sorglose Umgang mit Daten, die Sammelleidenschaft von Unternehmen und der Wunsch, aus der Datenflut automatisiert Schlüsse auf die Kaufgewohnheiten der Kunden zu ziehen – das alles erwog die europäische Kommission dazu, ein europaweit einheitliches und hohes Niveau an Datenschutz etablieren zu wollen. Das Ergebnis dieser Anstrengungen ist die EU-Datenschutzgrundverordnung.

Das Thema Datenschutz geht Hand in Hand mit technischen und organisatorischen Maßnahmen, um ein Schutzniveau zu garantieren und gegenüber Dritten nachweisbar zu machen. Deswegen hat sich auch der IT-Cluster mit dem Information Security Network (ISN) den Themen Informationssicherheit und Datenschutz verschrieben.

Das ISN betreibt Aufklärungsarbeit und vermittelt durch ExpertInnen den angemessenen und vernünftigen Umgang mit der neuen Verordnung. Darüber hinaus können Unternehmen auf der Suche nach Lösungen für ihre Herausforderungen kostenlos Orientierungshilfe in Anspruch nehmen.

www.itcluster.at

HIGHLIGHTS 2018

08. FEBRUAR 2018
Auftaktveranstaltung der Softwarepark Hagenberg
IT-ExpertInnenreihe Information Security
FH OÖ Campus Hagenberg

13. APRIL 2018
Lange Nacht der Forschung 2018
IT-Center, amsec IMPULS

02.-03. MAI 2018
Security Forum 2018
FH OÖ Campus Hagenberg

21. JUNI 2018
2. Veranstaltung der Softwarepark Hagenberg
IT-ExpertInnenreihe Information Security
amsec IMPULS

16.-18. JULI 2018
Kinderuni Hagenberg
FH OÖ Campus Hagenberg

15.-31. AUGUST 2018
Europäisches Forum Alpbach 2018
Alpach, Tirol
Terminübersicht siehe www.alpbach.org

16.-17. OKTOBER 2018
IKT-Sicherheitskonferenz 2018
Congress Centrum Alpbach, Tirol

18. OKTOBER 2018
Karrieremesse FH>>next für IT und Medien
FH OÖ Campus Hagenberg

22. NOVEMBER 2018
3. Veranstaltung der Softwarepark Hagenberg
IT-ExpertInnenreihe Information Security
Schloss Hagenberg

VIELE WEITERE VERANSTALTUNGEN
www.softwarepark-hagenberg.com/veranstaltungen

IMPRESSUM & OFFENLEGUNG GEM. § 25 MEDIENGESETZ
Blattlinie: Information über aktuelle Entwicklungen im Bereich der IT-Industrie. Das Magazin erscheint jährlich. Der Softwarepark Hagenberg ist eine Initiative des Landes Oberösterreich und ein Spin-off der Johannes Kepler Universität. Träger des Softwarepark Hagenberg ist die Business Upper Austria – OÖ Wirtschaftsagentur GmbH.
Medieninhaber (Verleger) und Herausgeber: Business Upper Austria – OÖ Wirtschaftsagentur GmbH, Redaktionsadresse: Hauptstraße 90, 4232 Hagenberg, Telefon: +43 7236 3343 0, Fax: +43 7236 3343 590, E-Mail: office@softwarepark-hagenberg.com, www.softwarepark-hagenberg.com. Für den Inhalt verantwortlich: DI (FH) Werner Pamminger, MBA. Redaktion: Dr. Sonja Mündl. Umsetzung Grafik: Agentur Sara Aschauer, MA, BSc, www.sarai-creations.com. Bildmaterial: Titelbild: jijomathaidesigners/Shutterstock.com. Alle anderen Bilder, wenn nicht anders angegeben: Softwarepark Hagenberg. Gastbeiträge müssen nicht notwendigerweise die Meinung des Herausgebers wiedergeben. Beigelegte Unterlagen stellen entgeltliche Informationsarbeit des Softwarepark Hagenberg für die Partner dar. Alle Angaben erfolgen trotz sorgfältiger Bearbeitung ohne Gewähr; eine Haftung ist ausgeschlossen.

Aufgrund des besseren Leseflusses wurde beim Verfassen teilweise auf explizites Gendern verzichtet. Sämtliche Formulierungen umfassen beide Geschlechter.

softwarepark hagenberg
business research education

your networking site

WHERE IDEAS TURN INTO SUCCESS

www.softwarepark-hagenberg.com