

**PRESSEINFORMATION**

**Buch: IT-Sicherheit in der Beschaffung**

Ratgeber für Organisationen, Unternehmen und Haushalte

**Wer Produkte mit integrierter Software kauft, kauft das Problem mitunter schon mit: Unsichere Komponenten in Produkten können sich für viele Unternehmen später als Problem herausstellen. Während auf Rechnern meist Sicherheitsprogramme installiert werden und sich IT-Abteilungen mit Firewalls und anderen Maßnahmen um die Sicherheit kümmern, werden Gefahren durch Software und Geräte beim Einkauf meist nicht berücksichtigt. Das Buch „Beschaffung unter Berücksichtigung der IT-Sicherheit“ bietet Hilfe für Einkäuferinnen und Einkäufer.**

**St. Pölten, 12.07.2017** – IT-Sicherheit betrifft keineswegs nur Produkte wie Computer und Software. Auch bei Gegenständen, wo es auf den ersten Blick nicht so ersichtlich ist, spielt sie durch die eingebauten Komponenten an Hard- und Software eine Rolle, zum Beispiel bei Kameras, Staubsaugerrobotern, Autos oder Fernsehern. Zudem sind im Zeitalter des „Internets der Dinge“ (Internet of Things, IoT) immer mehr Geräte, die im Alltag und in Unternehmen benutzt werden, mit dem Internet verbunden.

Vergangenes Jahr hat die FH St. Pölten die Plattform „www.it-sicher.kaufen“ gestartet. Sie liefert kostenlos und unabhängig von Herstellerinnen und Herstellern Sicherheits-Checklisten passend zu individuellen Ansprüchen. Nun hat Ernst Piller, Leiter des Instituts für IT Sicherheitsforschung an der FH St. Pölten, ein Buch zum Thema veröffentlicht.

„Preis, Funktion und Design spielen beim Einkauf von Produkten oft die größte Rolle. Kaum jemand schaut auf die IT-Sicherheit. Die beginnt aber bereits beim Einkauf“, sagt Piller. IT-Sicherheit wird laut Piller beim Einkauf nur in größerem Umfang beachtet, wenn sie gesetzlich vorgeschrieben ist: etwa im Gesundheitsbereich mit sensiblen und medizinischen Daten.

**Beschaffung unter Berücksichtigung der IT-Sicherheit**

Im Buch zeigt Piller die Wichtigkeit der IT-Sicherheit bei der Beschaffung jeglicher Software und Hardware für die IT-Sicherheit der eigenen Infrastruktur bzw. für in Produktionsunternehmen hergestellte Produkte auf. Zu Hardware zählen neben IKT-Produkten auch alle Geräte, Maschinen, Steuerungen, Fahrzeuge etc., die Software enthalten.

Piller beschreibt für BeschafferInnen und EinkäuferInnen Herausforderungen, Maßnahmen, IT-Sicherheitsanforderungen und Prozessschritte, um IT-Sicherheit bestmöglich in den Beschaffungsprozess zu integrieren. Dabei werden auch Themen wie Vertrauen in HerstellerInnen, beschaffungsrelevante Informationssysteme für IT-Sicherheit und Gütezeichen behandelt.

Zielgruppe für das Buch sind Personen, die Software jeglicher Art oder Hardware-Produkte mit integrierter (embedded) Software einkaufen – in Organisationen oder Industrieunternehmen, die Komponenten mit integrierter Software verarbeiten bzw. Software für ihre Produkte extern entwickeln lassen, Handelsunternehmen für die Beschaffung von Handelswaren und Menschen, die sich für IT-Sicherheit beim privaten Einkauf interessieren.

**Vertrauen zwischen Handel und Kundschaft**

Einerseits sollen HerstellerInnen, AnbieterInnen, HändlerInnen sowie Lieferantinnen und Lieferanten ihren Kundinnen und Kunden garantieren können, dass die angebotene Hardware und Software ordnungsgemäß funktioniert, die relevanten und wichtigen IT-Sicherheitsanforderungen erfüllt und keine Fehler oder Schwachstellen besitzt. Andererseits müssen Kundinnen und Kunden im Rahmen einer „IT-sicheren Beschaffung“ darauf achten, dass die erworbenen Produkte IT-sicher und vertrauenswürdig sind und nur die gewünschten Funktionalitäten enthalten.

IT-Sicherheit komme im Beschaffungsprozess jedoch oftmals nur sehr eingeschränkt vor und fehle weitestgehend in der Beschaffungsliteratur. „Etwas Unsicheres zu kaufen kann später sehr teuer werden. Diese Botschaft ist vielen Beschafferinnen und Beschaffern noch nicht bewusst, vor allem in KMUs“, erklärt Piller.

**Buch:** Ernst Piller: Beschaffung unter Berücksichtigung der IT-Sicherheit. Wichtigkeit, Herausforderungen und Maßnahmen. Springer Vieweg 2017

ISBN/EAN: 9783658185992

E-Book: 4,99 €, Softcover: 10,27 €

<http://www.springer.com/de/book/9783658185985>

**Autor:** Ernst Piller ist Informatiker, Leiter des Instituts für IT-Sicherheitsforschung an der FH St. Pölten, Universitätsdozent an der TU Wien und IT-Sicherheitsberater.

**Plattform „it-sicher.kaufen:**

Die Plattform ist Teil und Ergebnis des Forschungsprojekts ITsec.at, das sich mit Gefahren durch Angriffe aus dem Cyberraum für die österreichische Informations- und Kommunikationstechnik befasste und Strategien, Vorgehensempfehlungen und Sicherheitstests erforschte. Partner im Projekt waren die SEC Consult Unternehmensberatung GmbH, das Bundeskanzleramt, das Bundesministerium für Inneres, das Bundesministerium für Landesverteidigung und Sport und das Magistrat der Stadt Wien (MA14, Informations- und Telekommunikationssysteme). Finanziert wurde das Projekt vom Bundesministerium für Verkehr, Innovation und Technologie im Rahmen der FFG-Programmlinie KIRAS (Sicherheitsforschung).

[www.it-sicher.kaufen](http://www.it-sicher.kaufen)

**Fotos:**

Buchcover, Credit: Springer Vieweg

Porträt Ernst Piller, Credit: privat

Symbolbild IT, Credit: FH St. Pölten

FH St. Pölten, Credit: Martin Lifka Photography

**Über die Fachhochschule St. Pölten**

Die Fachhochschule St. Pölten ist Anbieterin praxisbezogener und leistungsorientierter Hochschulausbildung in den sechs Themengebieten Medien & Wirtschaft, Medien & Digitale Technologien, Informatik & Security, Bahntechnologie & Mobilität, Gesundheit und Soziales. In mittlerweile 17 Studiengängen werden rund 2.880 Studierende betreut. Neben der Lehre widmet sich die FH St. Pölten intensiv der Forschung. Die wissenschaftliche Arbeit erfolgt zu den oben genannten Themen sowie institutsübergreifend und interdisziplinär. Die Studiengänge stehen in stetigem Austausch mit den Instituten, die laufend praxisnahe und anwendungsorientierte Forschungsprojekte entwickeln und umsetzen.

**Informationen und Rückfragen:**

Mag. Mark Hammer

Marketing und Unternehmenskommunikation

T: +43/2742/313 228 269

M: +43/676/847 228 269

E: [mark.hammer@fhstp.ac.at](mailto:mark.hammer@fhstp.ac.at)

I: <https://www.fhstp.ac.at/de/presse>

Pressetext und Fotos zum Download verfügbar unter <https://www.fhstp.ac.at/de/presse>.

Allgemeine Pressefotos zum Download verfügbar unter <https://www.fhstp.ac.at/de/presse/pressefotos-logos>.

Natürlich finden Sie uns auch auf Facebook und Twitter: [www.facebook.com/fhstp](http://www.facebook.com/fhstp), [https://twitter.com/FH**\_**StPoelten](https://twitter.com/FH_StPoelten).

Sollten Sie in Zukunft keine weiteren Zusendungen der Fachhochschule St. Pölten wünschen, senden Sie bitte ein Mail mit dem Betreff „Keine Presseaussendungen" an [presse@fhstp.ac.at](mailto:presse@fhstp.ac.at).