ÖFIT-Trendschau

Öffentliche Informationstechnologie in der digitalisierten Gesellschaft

Trendthema 23:

Security by Design

Stand: Juli 2016

Herausgeber:
Mike Weber
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut FOKUS
Kaiserin-Augusta-Allee 31, D-10589 Berlin
Telefon: +49 30 3463 - 7173
Telefax: + 49 30 3463 - 99 - 7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

Autorinnen und Autoren der Gesamtausgabe:
Mike Weber, Stephan Gauch, Faruch Amini, Tristan Kaiser, Jens Tiemann, Carsten Schmoll, Lutz Henckel, Gabriele Goldacker, Petra Hoepner, Nadja Menz, Maximilian Schmidt, Michael Stemmer, Florian Weigand, Christian Welzel, Jonas Pattberg, Nicole Opiela, Florian Friederici, Jan Gottschick, Jens Fromm

Autorinnen und Autoren einzelner Trendthemen:
Michael Rothe, Oliver Schmidt

ISBN: 978-3-9816025-2-4

Juli 2016

Autorinnen/Autoren:
Nadja Menz et al.

Bibliographische Angabe:
Nadja Menz et al. 2019, Security by Design, In: Jens Fromm und Mike Weber, Hg., 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, http://www.oeffentliche-it.de/-/security-by-design

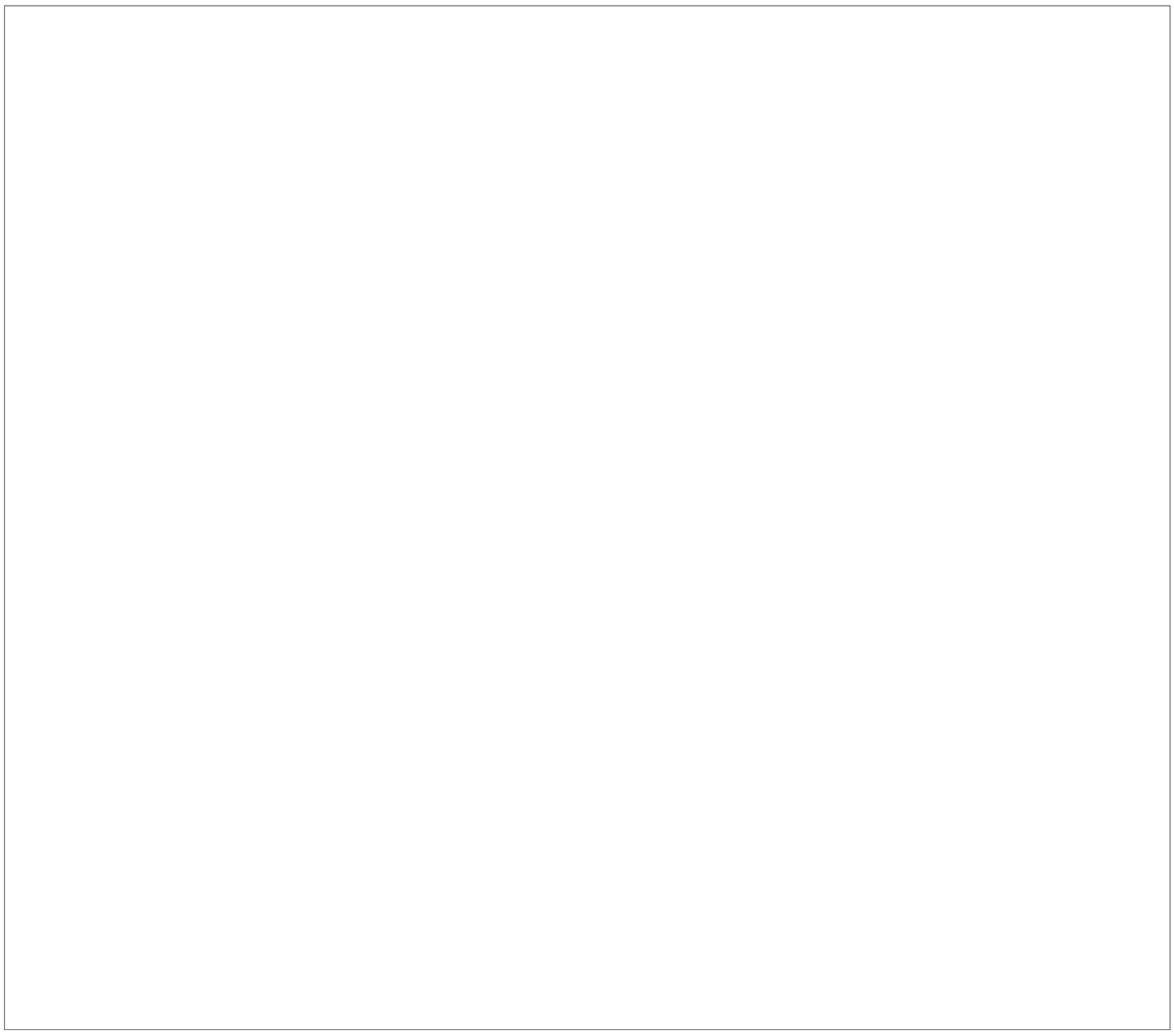
Security by Design

Datendiebstahl, Cyberattacken und Online-Betrug bedrohen Bürger, Verwaltung und Wirtschaft. Durch die zunehmende Digitalisierung wird IT-Sicherheit so zu einem immer wichtigeren Thema für die Gesellschaft. Informationstechnische Sicherheitskonzepte setzten dabei oftmals erst am Ende von Prozessketten an. Security by Design ändert dies grundlegend, indem Sicherheitsaspekte als integraler Bestandteil in allen Phasen der Softwareentwicklung berücksichtigt werden, um Schwachstellen erst gar nicht entstehen zu lassen.

Integration von Sicherheit in die Softwareentwicklung

Anwendungen, die übertriebene Priorisierung von Funktionalität und Bequemlichkeit (siehe Usability) gegenüber der Sicherheit bei immer kürzeren Release-Zyklen aufweisen, und weitere Aspekte heutiger Softwareentwicklung (siehe Microservices) erhöhen die Angriffsfläche moderner Software ständig. Dass gängige, allerdings nur punktuell eingesetzte Sicherheitsmaßnahmen wie Penetrationstests und Quellcode-Reviews in den meisten Fällen nicht ausreichend sind, führen Nachrichten über ausgenutzte Software-Schwachstellen täglich neu vor Augen.
IT-Sicherheit kann nicht mehr nur als Add-On betrachtet werden. Security by Design versteht sich als Integration von Sicherheitsaspekten in alle Phasen der Softwareentwicklung – von der Anforderungsanalyse, über die Durchführung von Tests bis hin zur Inbetriebnahme beim Endkunden. Die Entstehung von Fehlern und Schwachstellen soll von vorneherein reduziert und eine integrierte und nachhaltige Sicherheit hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität erreicht werden.

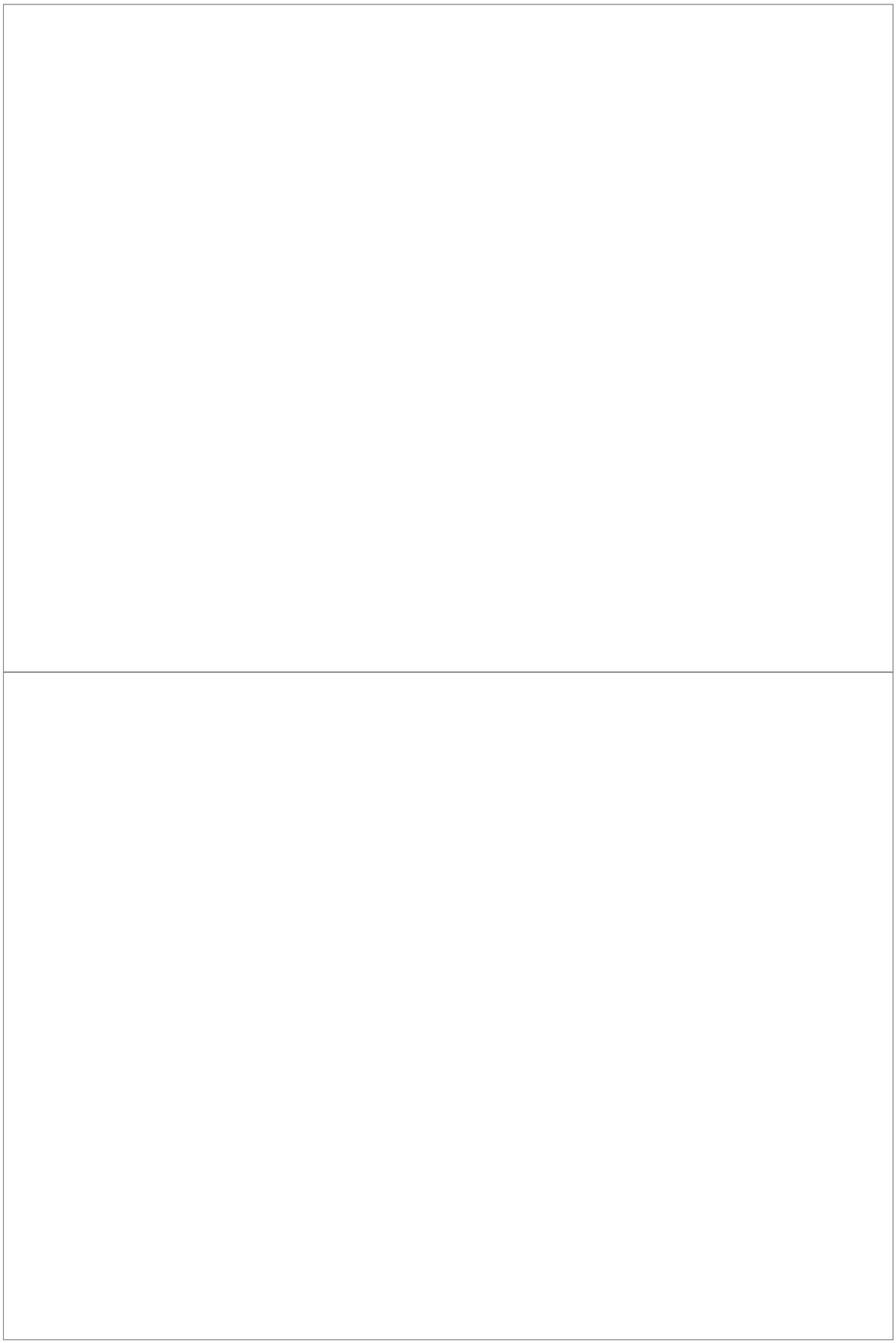
Begriffliche Verortung



Security by Design als Lösung für Schwachstellen

Häufig erfolgen Sicherheitsbewertungen und Penetrationstests erst am Ende einer Entwicklung, kurz vor der Auslieferung an den Kunden. Zu diesem Zeitpunkt bedeutet die Behebung von Schwachstellen jedoch bereits enorme zeitliche und finanzielle Aufwände. Noch schlimmer wiegen allerdings die Fälle, in denen Schwachstellen erst im laufenden Betrieb erkannt werden, sodass sich bis zum nächsten Sicherheitspatch ein in jedem Falle zu großes Zeitfenster öffnet, in dem die Software angegriffen werden kann. Je nach Anwendungsgebiet können Schaden für den Endanwender (siehe Digitale Unversehrtheit) und Rufschädigung des Herstellers beträchtlich ausfallen.
Mit dem Bedeutungszuwachs von IT-Sicherheit - vor allem in Hinblick auf Industrie 4.0 - findet Security by Design immer häufiger Erwähnung als möglicher Lösungsansatz. Schwachstellen der klassischen Softwareentwicklung haben bereits zur Übernahme einzelner Prinzipien von Security by Design durch zahlreiche Unternehmen geführt. Auch der gegenwärtige Paradigmenwechsel in der IT-Sicherheit begünstigt diese Entwicklung. Vollkommene Sicherheit kann es nach aktueller Auffassung nicht geben, respektive nicht mit angemessenem Aufwand erreicht werden. Vielmehr gilt es, Angriffe zu antizipieren und ihre Auswirkungen zu minimieren. Eine von Grund auf nach Sicherheitsaspekten entwickelte Software trägt hierzu entscheidend bei.

Themenkonjunkturen



Folgenabschätzung

Möglichkeiten

- IT-Sicherheit erfordert Ressourcen, die sich durch positive (Verkaufsargument) und Vermeidung negativer Effekte (Imageschaden) auch bei Herstellern mobilisieren lassen
- IT-Sicherheit ist ein internationaler Markt mit beträchtlichem Wachstumspotenzial, auf dem deutsche Unternehmen auch aufgrund der hohen deutschen Sicherheits- und Datenschutzanforderungen gute Chancen haben
- Initiale Kosten für die Integration von zusätzlichen Sicherheitsmaßnahmen können sich mittelfristig mehr als amortisieren

Wagnisse

- IT-Sicherheit wird mehr und mehr zur Bewertungs- und Abwägungsfrage, die allzu oft zu Gunsten von Funktionalität und Geschwindigkeit beantwortet wird.
- Hohe, anfängliche Mehrkosten einerseits gegenüber einer nicht zu beziffernden Erhöhung der Marktchancen andererseits kann zur Vernachlässigung von Sicherheitsaspekten im Entwicklungsprozess führen
- Hohe Startinvestitionen bei der Einführung von Security by Design Methoden schrecken insbesondere KMU ab
- Sicherheitsorientierte Softwareentwicklungsprozesse führen nicht zwangsläufig auch zu sicherer Software

Handlungsräume

IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz soll „zur Erhöhung der Sicherheit informationstechnischer Systeme" beitragen. Dabei wird ein Mindestniveau an IT-Sicherheit für kritische Infrastrukturen vorgesehen. Diese Ziele gilt es mit Leben zu füllen - Security by Design stellt hierfür eine Basismaßnahme dar.

Forschungsförderung

Das IT-Sicherheitsgesetz soll „zur Erhöhung der Sicherheit informationstechnischer Systeme" beitragen. Dabei wird ein Mindestniveau an IT-Sicherheit für kritische Infrastrukturen vorgesehen. Diese Ziele gilt es mit Leben zu füllen - Security by Design stellt hierfür eine Basismaßnahme dar.

Sicheres E-Government

Bei E-Government- und anderen IT-Projekten der öffentlichen Hand (siehe Verwaltung x.0) gilt es, mit gutem Beispiel voranzugehen und Sicherheitsinnovationen konsequent zur Anwendung zu bringen.