QualiCS-Kursprogramm

Hintergrund

Die zunehmende digitale Vernetzung und der daraus folgende Qualifizierungsbedarf sind auch im Life-Science-Bereich zu beobachten. IT-Sicherheit ist für alle Unternehmen im Life-Science-Bereich relevant. Mit zunehmender Bedeutung von Cloud Computing und neuen Möglichkeiten der Datengenerierung und -auswertung steigen die Anforderungen an den Schutz von vernetzten Instrumenten und Techniken, Steuerungsanlagen, Innovationsideen und (Patienten-)Daten.

Im Rahmen des Projektes QualiCS wird ein an die **Bedarfe von KMU** in Schleswig-Holstein angepasstes Qualifizierungsprogramms zum Thema IT-Sicherheit für Beschäftigte des Life-Science-Clusters entwickelt. Das Weiterbildungsangebot unterstützt Beschäftigte durch den Aufbau von Wissen, Fähigkeiten und Kompetenzen darin, **mit den technischen Entwicklungen Schritt zu halten**. Dadurch wird ein Beitrag zur Stärkung der KMU und der Region sowie für die Weiterentwicklung von Fachpersonal geleistet.

Beginn der Erprobungsphase am 1. Juli 2018

Ab 1. Juli 2018 können Mitarbeitende von Kleinst-, Klein- und mittleren Unternehmen der Life- Science-Branche mit Sitz in Schleswig-Holstein die entwickelten Module kostenfrei testen. Informationen zum Programm und Anmeldehinweise finden Sie auf: https://www.oncampus.de/qualics

Projektpartner

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

LIFE SCIENCE NORD

oncampus

Wir fördern Arbeit

EU.SH

Landesprogramm Arbeit: Gefördert durch die Europäische Union, Europäischer Sozialfonds (ESF), und das Land Schleswig-Holstein

Das Vorhaben QualiCS wird aus dem Landesprogramm Arbeit mit Mitteln des Europäischen Sozialfonds gefördert. Mehr Informationen im Internet: www.EU-SH.schleswig-holstein.de.

Grundlagenmodule

Awareness IT-Sicherheit **Autorin: Prof. Dr. Dorina Gumm**

Das Modul gibt einen Überblick über das breite Feld der IT-Sicherheit. Teilnehmende erhalten einen Einblick in die Relevanz der Thematik für Unternehmen und die Gesellschaft im Allgemeinen, lernen die wichtigsten Angriffsszenarien kennen und erfahren, wie sie sich mit einfach umsetzbaren Maßnahmen schützen können. (Lernumfang: 10 h)

Passwortsicherheit **Autorin: Prof. Dr. Dorina Gumm**

Dieses Modul beschäftigt sich mit der Frage, wie Passwörter sicher gestaltet werden können. Hierfür lernen die Teilnehmenden verschiedene Möglichkeiten kennen, wie Passwörter herausgefunden werden können, sie beschäftigen sich mit Qualitätskriterien für Passwörter und werden in die Lage versetzt, ihre Passwörter sicherer zu gestalten. (Lernumfang: 2 h)

IT-Sicherheitstools **Autor: Prof. Dr. Andreas Hanemann**

In diesem Grundlagenkurs werden IT-Sicherheits-Tools vorgestellt, die auf Testwebsites ausprobiert werden können. Webauftritt, Geräte- und Webserverkonfiguration werden dabei genauso betrachtet wie das sichere Bewegen im Internet. Teilnehmende wissen hiernach, ob ein Tool für ihr Unternehmen geeignet ist und wie es implementiert werden kann. (Lernumfang: 15 h)

Sicherheit mobiler Endgeräte **Autor: Michael Sendke**

In diesem Modul erhalten die Teilnehmenden Basiswissen über die Nutzung mobiler Endgeräte und Netzwerke. Dabei wird u.a. auf die grundlegenden technischen Möglichkeiten zum Schutz von Mobilgeräten eingegangen, Sicherheitsgefahren beim Empfang von neuen und der Abgabe von alten Geräten verdeutlicht und datenschutzrelevante Aspekte behandelt. (Lernumfang: 2 h)

Datensicherheit auf Reisen **Autor: Michael Sendke**

In der U-Bahn, im Zug, in Restaurants oder auf dem Bahnsteig, überall begleiten uns Notebooks, Smartphones oder Tablets und sorgen so für eine ständige Erreichbarkeit und Verfügbarkeit von Daten und E-Mails. Dieses Modul gibt Antworten auf die Fragen, wo die größten Gefahren bei der Gerätenutzung auf Reisen liegen und wie man sich auf einfache Art und Weise schützen kann. (Lernumfang: 2 h)

Social Engineering **Autor: Hannes Molsen**

Social Engineering ist die gefährlichste Form des Informationsdiebstahls und der Manipulation. Die ausgenutzte Schwachstelle, der Mensch, kann nicht durch Firewalls oder Antivirensoftware geschützt werden. In diesem Modul werden Empfehlungen für einen bewussten Umgang mit vertraulichen Daten am PC, am Telefon und in sozialen Netzwerken gegeben, um Social-Engineering-Angriffen entgegenzutreten. (Lernumfang: 2 h)

Datensicherung – Notwendigkeiten und Möglichkeiten **Autor: Volker Haseldiek**

In jedem Unternehmen werden digitale Rechensysteme und ggf. mobile Endgeräte zur Erfassung, Speicherung und Verarbeitung von Daten verwendet. Dieses Modul zeigt verschiedene Möglichkeiten der Datensicherung, darunter auch cloudbasierte Abwendungen, auf und gibt Hinweise, wie ungewollte Veränderungen oder der Verlust von Daten vermieden werden können. (Lernumfang: 2 h)

Aufbaumodule

Informationssicherheitsmanagement **Autor: Michael Wiesner**

Das Modul gibt sowohl einen Überblick über die Bestandteile eines Informationsmanagementsystems wie auch praktische Anleitungen, wie KMU ein solches implementieren können. Grundlage der Empfehlungen ist die auf KMU ausgerichtete VdS-Richtlinie 3473. (Lernumfang: 10 h)

Netzwerksicherheit **Autor: Daniel Theuermann**

Das Verständnis von Sicherheit und Angriffs- und Abwehrmechanismen auf Netzwerkebene stellt ein grundlegendes Element zur wirksamen Absicherung gegen IT-Angriffe dar. Teilnehmende lernen Angriffsarten und Vorgehen bei Angriffen im Netzwerk, Strategien und Technologien zur Abwehr und Kriterien zum Assessment des eigenen Unternehmensnetzwerkes kennen. (Lernumfang: 15 h)

Rechtliche Grundlagen der Informationssicherheit **Autor: Michael Wiesner**

In diesem Modul werden rechtliche Grundlagen und Anforderungen an die unternehmenseigene IT-Sicherheit präsentiert, die Unternehmen berücksichtigen müssen. Dabei wird auf die maßgeblichen Gesetze, Verordnungen und Richtlinien eingegangen. (Lernumfang: 2 h)

Datenschutzgrundverordnung **Autor: Hans-Dieter Neumann**

Die europäische Datenschutzgrundverordnung (EU-DSGVO) ruft bei Unternehmen einen umfassenden Handlungsbedarf hervor. Grund sind die faktische Beweislastumkehr und drastische Bußgelderhöhungen bei Nicht-Einhaltung ab dem 25.05.2018. Teilnehmende erhalten aktuelle Informationen und können die notwendigen Schritte zur Umsetzung einleiten. (Lernumfang: 10 h)

Entwicklung sicherer Produkte **Autor: Hannes Molsen**

– Teil I: Einführung und Entwicklungslebenszyklen

Dieses Modul ist eine Einführung in die Entwicklung IT-sicherer Produkte und den damit verbundenen Entwicklungslebenszyklus. Teilnehmende lernen die IT-relevanten Teilbereiche des Produktlebens kennen und werden sich der Wichtigkeit einer ganzheitlichen Betrachtung von IT-Sicherheit bewusst. (Lernumfang: 5 h)

– Teil II: Sichere Architekturen

Sicherheitslücken können in jeder Phase einer Produktentwicklung auftreten. Fehler in der Produktarchitektur sind jedoch gravierend und häufig nur sehr schwer und teuer zu beheben. In diesem Modul beschäftigen sich die Teilnehmenden mit Systemanforderungen an IT-Sicherheit, Kryptografie, Architekturmustern und -prinzipien und können eine Bedrohungsanalyse durchführen. (Lernumfang: 5 h)

– Teil III: Sicheres Entwickeln und Testen

Viele Sicherheitslücken in der Produktentwicklung entstehen während der Programmierung. In diesem Modul werden die gängigsten Sicherheitslücken in der Entwicklung thematisiert und Methoden vorgestellt, um Produkte auf Sicherheit zu testen. (Lernumfang: 5 h)

– Teil IV: Software-Wartung und Verwaltung von Software-Komponenten

Eine effiziente Wartung externer Softwarekomponenten ist von großer Bedeutung für die IT-Sicherheit. Teilnehmende lernen Methoden kennen, um die Qualität von Komponenten einzuschätzen, erhalten Quellenhinweise für Sicherheitsrisiken und werden in die Lage versetzt, Sicherheitsrisiken professionell abzuarbeiten. (Lernumfang: 2 h)

IT-Notfallmanagement für KMU in den Life Sciences **Autorin: Stephanie Ewe**

Mit einem IT-Notfallmanagement können Unternehmen Vorkehrungen für den Fall eines Angriffs auf ihre IT-Infrastrukturen oder Produkte treffen. Das Modul unterstützt Teilnehmende dabei, den konkreten Bedarf für Notfallmanagement zu identifizieren und relevante Notfallmaßnahmen festzulegen. (Lernumfang: 10 h)

Regulatorische Aspekte der IT-Sicherheit von Medizinprodukten **Autor: Norbert Pauli**

Für die Zulassung von Medizinprodukten gibt es auch regulatorische Anforderungen an die IT-Sicherheit. In diesem Modul lernen Teilnehmende die zentralen Gesetze und Normen hierzu kennen und können einschätzen, wie diese sich auf die unternehmenseigenen Geschäftsbereiche und Prozesse auswirken. (Lernumfang: 5 h)

IT-Sicherheit von Medizinprodukten (engl.) **Autor: Hannes Molsen**

Dieses Modul vermittelt umfassende Kenntnisse in der Entwicklung IT-sicherer Medizinprodukte einschließlich der rechtlichen und regulatorischen Anforderungen und dem daraus resultierenden und nötigen Entwicklungslebenszyklus. Das Modul wird in englischer Sprache angeboten. (Lernumfang: 15 h)

Patientendaten in klinischen Studien sicher verarbeiten **Autorin: Stephanie Ewe**

Für die Verwendung von Patientendaten in klinischen Studien gibt es spezifische regulatorische Anforderungen. Teilnehmende lernen diese kennen sowie beschäftigen sich mit dem Lifecycle der Datenverarbeitung und den organisationalen Voraussetzung der sicheren Verarbeitung von Patientendaten. Datenschutz- und datensicherheitsrelevante Aspekte werden thematisiert. (Lernumfang: 15 h)