

Cybersecurity Essentials



Kurs starten



Ressourcen für Kursteilnehmer



Wissensquiz zum Kurs

Autoren: Michael Zeisberger
Instruktor der Cisco Networking Academy

Inhalt

- Übersicht der Kursinhalte
- Navigationsmöglichkeiten
- Suchmöglichkeiten im Kurs
- Das Zertifikat zum Kurs
- Anregungen zur Einführung ins Thema

Kursinhalte (1/4)

Kapitel 1

Verhalten von Kriminellen und Spezialisten im „Cybersecurity-Raum“

Abschnitt 1.0
Einführung

Abschnitt 1.1
Die Welt der Cybersicherheit

Abschnitt 1.2
Cyberkriminelle gegen Cyberhelden

Abschnitt 1.3
Bedrohungen im Cyberraum

Abschnitt 1.4
Verbreitung und Vorgehen der Cyberkriminellen

Abschnitt 1.5
Cyberexperten - Organisationen, Zertifizierungen

Abschnitt 1.6
Zusammenfassung

Kapitel 2

Vertraulichkeit, Integrität und Verfügbarkeit von Daten

Abschnitt 2.0
Einführung

Abschnitt 2.1
Dimensionen der Cybersicherheit

Abschnitt 2.2
Das „CIA“-Dreieck

Abschnitt 2.3
Datenzustände

Abschnitt 2.4
Cybersicherheitsmaßnahmen

Abschnitt 2.5
Das ISO-Cybersicherheitsmodell

Abschnitt 2.6
Zusammenfassung

Kapitel 3

Schwerpunkte der Cyberkriminellen

Abschnitt 3.0
Einführung

Abschnitt 3.1
Maleware und Schadcode

Abschnitt 3.2
Angriffsmethode - Täuschung

Abschnitt 3.3
Weitere Angriffsmethoden

Abschnitt 3.4
Zusammenfassung

Kursinhalte (2/4)

Kapitel 4 Schutz der Vertraulichkeit

Abschnitt 4.0
Einführung

Abschnitt 4.1
Kryptografie

Abschnitt 4.2
Zugriffskontrolllisten

Abschnitt 4.3
Verschleiern von Daten

Abschnitt 4.4
Zusammenfassung

Kapitel 5 Datenintegrität

Abschnitt 5.0
Einführung

Abschnitt 5.1
Kontrollen für die Daten-
integrität

Abschnitt 5.2
Digitale Signaturen

Abschnitt 5.3
Zertifikate

Abschnitt 5.4
Datenbankintegrität

Abschnitt 5.5
Zusammenfassung

Kapitel 6 Sicherstellung hoher Verfügbarkeit

Abschnitt 5.0
Einführung

Abschnitt 5.1
Die „Five Nines“

Abschnitt 5.2
Steigern der Verfügbarkeit

Abschnitt 5.3
Reaktionen auf Sicherheits-
vorfälle

Abschnitt 5.4
Disaster Recovery

Abschnitt 5.5
Zusammenfassung

Kursinhalte (3/4)

Kapitel 7

Schutzmaßnahmen für Netzwerkkomponenten

Abschnitt 7.0
Einführung

Abschnitt 7.1
Verteidigung von Systemen und Geräten

Abschnitt 7.2
Serverabsicherung

Abschnitt 7.3
Netzwerkabsicherung

Abschnitt 7.4
Physische Sicherung

Abschnitt 7.5
Zusammenfassung

Kapitel 8

Stellschrauben der Cybersecurity-Bereiche

Abschnitt 8.0
Einführung

Abschnitt 8.1
Bereiche Cybersicherheit

Abschnitt 8.2
Ethik, Gesetze, Haftung

Abschnitt 8.3
Berufe in der Cybersicherheit

Abschnitt 8.4
Zusammenfassung

Kursinhalte (4/4)

Übungen

zu Kapitel 1

- Cybersicherheit - Stellensuche
- Identifikation von Sicherheitsrisiken
- Analyse des Berufsfeldes von Cybersicherheitsexperten

zu Kapitel 2

- Installieren einer virtuellen Maschine auf einem PC
- Arbeiten mit Authentifizierung, Autorisierung und Accounting

zu Kapitel 3

- Bedrohungen und Sicherheitslücken erkennen

zu Kapitel 4

- Verwenden von Steganografie

zu Kapitel 5

- Kennwortknacken
- Digitale Signaturen
- Sicherer Remote-Zugriff

zu Kapitel 7

- Absichern eines Linux-Systems

Navigationsmöglichkeiten - Kurs-Startseite (1/5)

Startseite

Module

Diskussionen

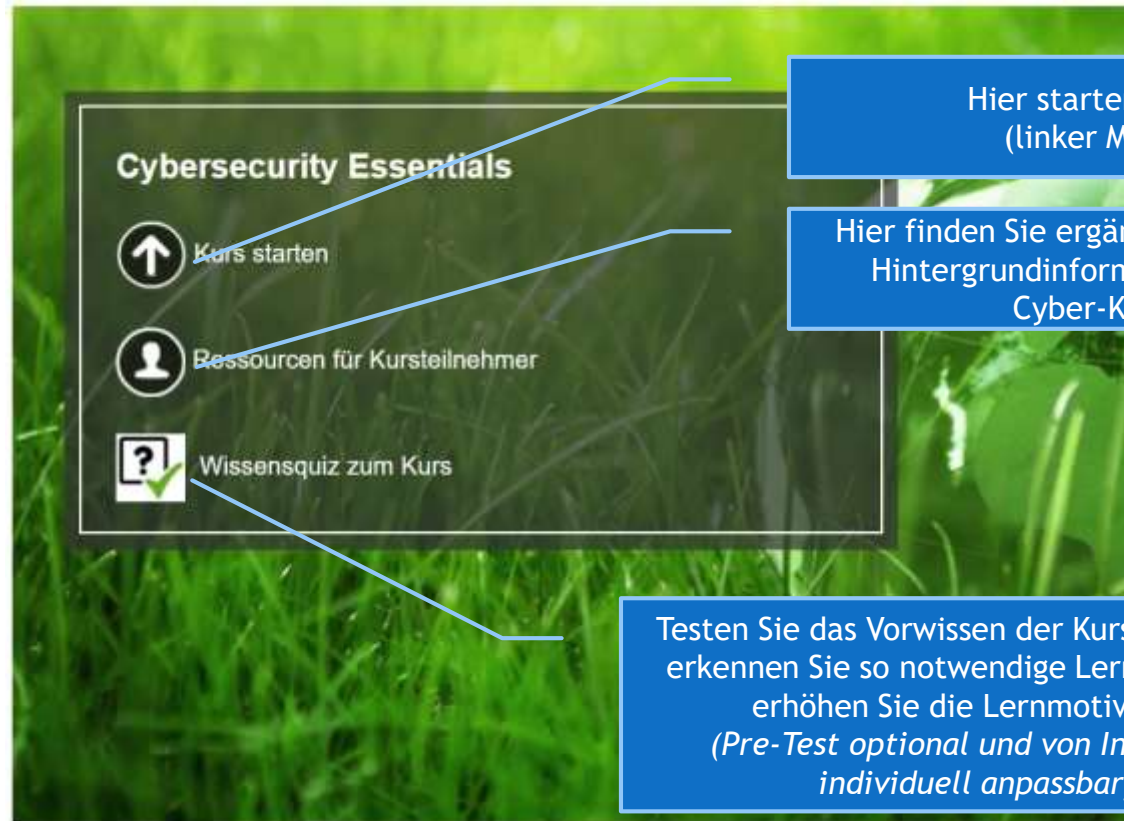
Noten

Aufgaben

Quizzes

Kollaboration

Von Instructor vergebener Name des Kurse



Hier starten Sie den Kurs
(linker Mouse-Klick)

Hier finden Sie ergänzende Dokumente und
Hintergrundinformationen zum Thema
Cyber-Kriminalität

Testen Sie das Vorwissen der Kursteilnehmer,
erkennen Sie so notwendige Lernfelder und
erhöhen Sie die Lernmotivation
(Pre-Test optional und von Instructor
individuell anpassbar)

Navigationsmöglichkeiten - Kurs-Startseite (2/5)

The image shows a course start page interface. On the left, there is a vertical navigation menu with the following items: Startseite (highlighted in blue), Module, Diskussionen, Noten, Aufgaben, Quizzes, and Kollaboration. At the top right, there is a header box containing the text "Von Instrutor vergebener Name des Kurse". The main content area features a green background with a globe and a sidebar menu with icons for "Cybers", "Ku", "Re", and "W". Three blue callout boxes provide detailed information about these icons: the top one points to the "Cybers" icon, the middle one to the "Ku" icon, and the bottom one to the "W" icon.

Startseite

Von Instrutor vergebener Name des Kurse

Module

Diskussionen

Noten

Aufgaben

Quizzes

Kollaboration

Cybers

Ku

Re

W

Direktzugriff auf alle Kurselemente, einschließlich ‚Final Exam‘ (Instruktoren können hierüber auch die Kursinhalte konfigurieren)

Kursteilnehmer sehen hier die erzielten Ergebnisse für Quizzes und Final Exam (Instruktoren erhalten Einsicht in die Lernerfolge aller Teilnehmer im Kurs)

Direktzugriff auf die kapitelspezifischen Quizzes im Kurs (Instruktoren können hier auch eigene Quizzes anlegen)

Navigationsmöglichkeiten im Kurs (3/5)

Cybersecurity Essentials – Grundlagen der Cybersicherheit

Kapitel 0
Kurs Einführung

Kapitel 1
Cybersicherheit – eine Welt von Hackern, Hacked und Kriminellen

Kapitel 2
Der Hexenwälder-Würfel der Cybersicherheit

Kapitel 3
Cybersicherheitsbedrohungen, Sicherheitsdaten und Angriffe

Kapitel 4
Die Kunst, Gefahrenrisiko zu schützen

Kapitel 5
Die Kunst, Integrität zu gewährleisten

Kapitel 6
99,999 % - Hochverfügbarkeit

Kapitel 7
Stärkung der Abwehr

Kapitel 8
Spezialtitel für Cybersicherheit werden

Abschnitt 2.0
Einführung

Abschnitt 2.1
Der Hexenwälder-Würfel der Cybersicherheit

Abschnitt 2.2
CIA-Dreieck

Abschnitt 2.3
Datensicherheit

Abschnitt 2.4
Cybersicherheitsmaßnahmen

Abschnitt 2.5
Framework für das Management der Informationssicherheit

Abschnitt 2.6
Zusammenfassung

Thema 2.2.1
Vertraulichkeit

Thema 2.2.2
Integrität

Thema 2.2.3
Verfügbarkeit

Seite 2.2.2.1
Das Prinzip der Datenintegrität

Seite 2.2.2.2
Bedarf an Datenintegrität

Seite 2.2.2.3
Integritätsprüfungen

Zuletzt besucht | Lesezeichen | Kurzanzeige | Suche | Sprachen | Hintergrund ändern | Hörs | Zurück zum Kurs

Steuern Sie mit der Mouse auf das gewünschte Kapitel und bestätigen Sie jeweils durch Klick der linken Mouse-Taste

Navigationsmöglichkeiten im Kurs (4/5)

Cybersecurity Essentials – Grundlagen der Cybersicherheit

Kapitel 2
Der Hasenmaister-Würfel der Cybersicherheit

2.1
Der Hasenmaister-Würfel der Cybersicherheit

2.1.1
Die drei Dimensionen

2.1.1.1
Sicherheitsprinzipien

Vertraulichkeit, Integrität und Verfügbarkeit

Informationszustände

Übertragung
Speicher
Verarbeitung

Vertraulichkeit
Integrität
Verfügbarkeit

Technologie
Richtlinien und Methoden
Personal

Gegenmaßnahmen

Sicherheitsprinzipien

Die erste Dimension des "Zauberwürfels" für die Cybersicherheit benennt die Ziele zum Schutz der Cybersicherheit. Sie ist in der ersten Dimension benannten Ziele handelt es sich um die grundlegenden Prinzipien der Cybersicherheit. Diese Prinzipien sind Vertraulichkeit, Integrität und Verfügbarkeit. Die Prinzipien schaffen einen Fokus und ermöglichen Cyberexperten eine Priorisierung von Aktionen zum Schutz der Cybersicherheit.

Vertraulichkeit ("C" im CIA-Dreieck, von Englisch "confidentiality") bedeutet, dass die Offenlegung von Informationen gegenüber nicht autorisierten Personen, Ressourcen oder Prozessen verhindert wird. Integrität ("I" im CIA-Dreieck, von Englisch "integrity") meint die Korrektheit, Konsistenz und Vertrauenswürdigkeit von Daten /Verfügbarkeit ("A" im CIA-Dreieck, von Englisch "availability") gewährleistet, dass autorisierte Benutzer Zugriff auf die Informationen haben, wann immer sie sie benötigen. Sie können sich dass die Prinzipien mit dem Akronym "VVI" merken.

Zuletzt besucht
Lesezeichen
Karte

Schließt den Abschnitt und führt zur Kapitelübersicht zurück

Setzen Sie Lesezeichen, um stimmte Stellen im Kurs zu markieren die später direkt aufrufbar sein sollen

Blättern Sie innerhalb des Abschnittes per Mouse-Klick (linke Taste) vor und zurück

Navigationsmöglichkeiten im Kurs (5/5)

Cybersecurity Essentials - Grundlagen der Cybersicherheit

Kapitel 0
Kursintroduction

Kapitel 1
Cybersicherheit - eine Welt von Helden, Kriminellen, Helden und Kriminellen

Kapitel 2
Der Heldenmeister-Würfel der Cybersicherheit

Kapitel 3
Cybersicherheitsbedrohungen, Sicherheitslücken und Angriffe

Kapitel 4
Die Kunst, Geheimnisse zu schützen

Kapitel 5
Die Kunst, Integrität zu gewährleisten

Kapitel 6
99,999 % - Hochverfügbarkeit

Kapitel 7
Stärkung der Abwehr

Kapitel 8
Spezialist für Cybersicherheit werden

Abschnitt 1.0
Einführung

Abschnitt 1.1
Die Welt der Cybersicherheit

Abschnitt 1.2
Cyberkriminelle gegen Cyberhelden

Abschnitt 1.3
Bedrohungen für das Königreich

Abschnitt 1.4
Die dunklen Mächte der Cybersicherheit

Abschnitt 1.5
Zeit für noch mehr Helden

Abschnitt 1.6
Zusammenfassung

Zuletzt Besucht | Lesezeichen | Menü/Index | Suche | Sprachen | Hintergrund ändern | Hilfe | Zurück zum Kurs

Direktzugriff auf zuvor markierte Textstellen im Kurs

Wählen Sie den gewünschten Lerninhalt direkt aus

Wechseln Sie mit zwei Klicks die Sprache

Führt Sie zurück zur Startseite


Suchmöglichkeiten im Kurs



Gewünschten Suchbegriff eingeben

Finden Sie die Textstellen im Kurs zu einem von Ihnen gesuchten Begriff

Das Zertifikat zum Kurs



Kursabschlusszertifikat

Ausgestellt für:

Vorname

über den erfolgreichen Abschluss des Kurses **Cisco Networking Academy® Cybersecurity Essentials** und zum Nachweis der folgenden Fähigkeiten:

- Beschreiben der Strategien, Techniken und Verfahren von Cyberkriminellen.
- Verständnis der Grundsätze von Vertraulichkeit, Integrität und Verfügbarkeit in Bezug auf Datenzustände und Gegenmaßnahmen.
- Darstellen der Technologien, Produkte und Verfahren, die zum Schutz der Vertraulichkeit, zur Sicherstellung der Integrität und zur Bereitstellung hoher Verfügbarkeit eingesetzt werden.
- Erläutern wie Cybersecurity-Experten Technologien, Prozesse und Verfahren einsetzen, um alle Komponenten des Netzwerks zu schützen.
- Erklären der Intention von Gesetzen im Zusammenhang mit Cybersecurity.

_____ Datum

Kursleiter

Unterschrift des Kursleiters

Nach erfolgreichem Absolvieren des ‚Final Exam‘ und Durchführung der Abschlußbefragung zum Kurs kann der Kursleiter (Instructor) für Teilnehmer ein Abschlußzertifikat erstellen

Anregungen zur Einführung ins Thema

Klären Sie die (Vor-)Kenntnisse Ihrer Schülerinnen und Schüler

Schaffen Sie Sensibilität für das Thema:

- zeigen Sie das Video von CompTIA: The most dangerous weapon ...‘
- zeigen Sie auf, in welchem Umfang heute Cyberkriminalität stattfindet
- lassen Sie die Schüler ihr individuelle Gefährdungspotenzial ermitteln

Cyberkriminalität findet nicht mehr nur per Malware statt

- verdeutlichen Sie die relevanten Dimensionen anhand des McCumber-“Würfels“

Führen Sie Ihre Schülerinnen und Schüler in den Kurs ein

- erläutern Sie Navigation und Bedienelemente
- sprechen Sie die Module an, die Sie im Kurs behandeln werden
- Erläutern Sie den von Ihnen vorgesehenen Kursablauf;
Bearbeitung der Module, geplante praktische Übungen, Leistungsnachweise

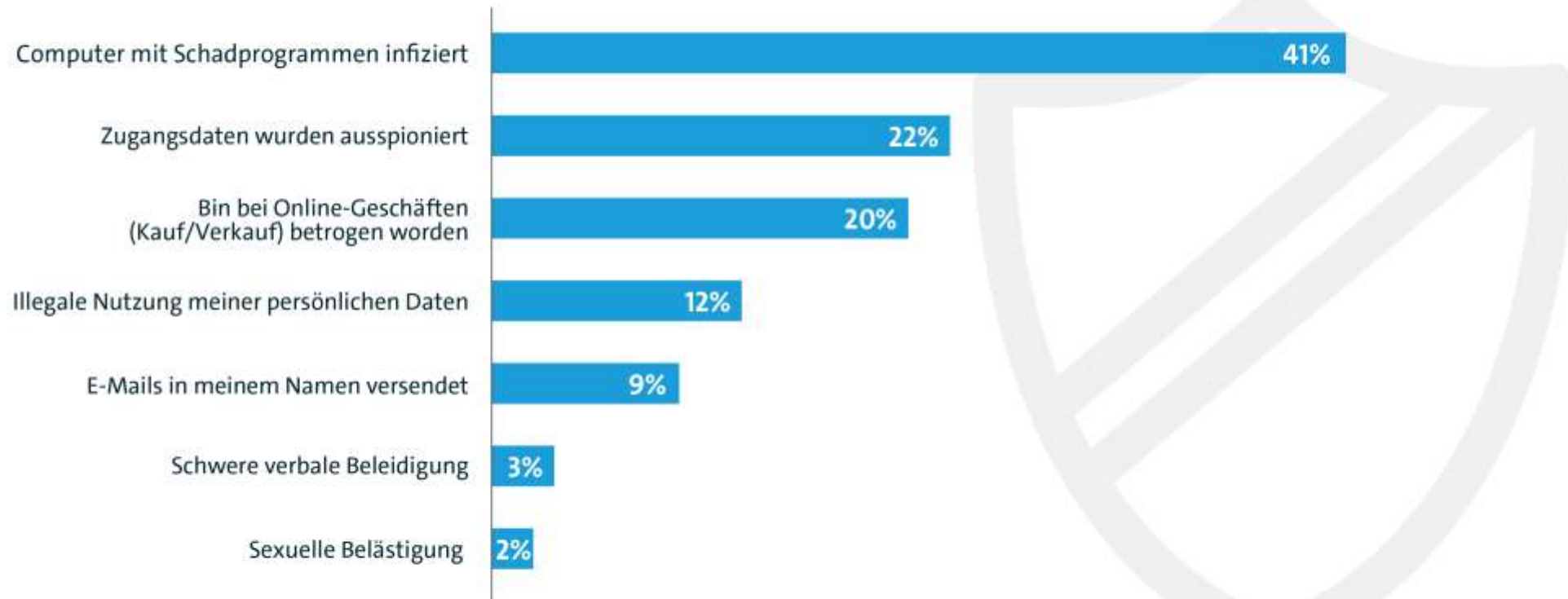
A person wearing a dark hoodie is centered in the frame, their face obscured by shadows. The background is a dark teal color filled with a dense pattern of white binary code (0s and 1s) and some small square icons, creating a digital or cyber-themed atmosphere.

Einführungsworkshop Cybersecurity Essentials

THE MOST DANGEROUS WEAPON IN THE WORLD

Viren, Betrug, Datenklau: Cybercrime trifft viele

Welche kriminellen Erfahrungen haben Sie in den vergangenen 12 Monaten im Internet gemacht?



Basis: Internetnutzer (n=1.017) | Mehrfachnennung möglich
Quelle: Bitkom Research 2016

Die größten Gefahren im Internet

Top 10 der größten Bedrohungen im Internet



Trojaner / Würmer



webbasierte
Schadsoftware



infizierte Websites /
mobile Apps



Botnetze



Denial-of-Service-
Attacken



Spam



Phishing



Viren-Baukästen



Physischer Verlust



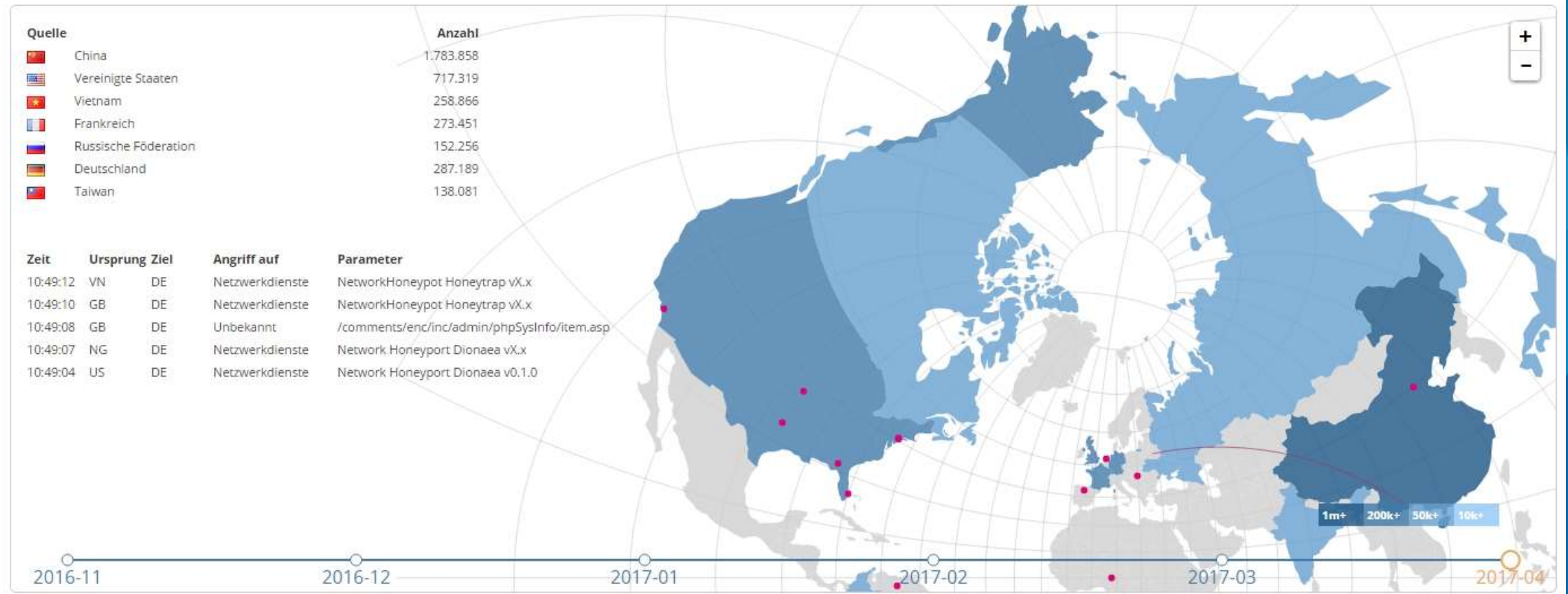
Datenverlust

Pfeile zeigen steigende bzw. sinkende Gefährdung
Quelle: ENISA, Bitkom

Live-Monitor von Cyber-Attacken im Internet

www.sicherheitstacho.eu

Übersicht über die aktuellen Cyberangriffe auf DTAG-Sensoren (aufgezeichnet von 180 Sensoren)



Cybercrime kommt Unternehmen teuer zu stehen

Durchschnittliche Schadenshöhe pro E-Crime-Fall bei Unternehmen in Deutschland (in Euro)



Dimensionen der Cybersicherheit

