ITSECURITY

Bavarian IT Security & Safety Cluster

ISIS12 - INFORMATIONSSICHERHEIT FÜR DEN MITTELSTAND

FELIX STRUVE
BAYERISCHEN IT-SICHERHEITSCLUSTER E.V.

REGENSTAUF, 31.03.2017


IT-SICHERHEIT IM MITTELSTAND

„Die eigenen Mitarbeiter sind die größte Schwachstelle“

18.09.2016 - Handelsblatt

Tesla-Crypt

Erpressung mit Trojaner - Stadtverwaltung zahlte Lösegeld

Ein Erpressungs-Trojaner hatte die Stadtverwaltung im unterfränkischen Dettelbach weitgehend lahmgelegt. Die Behörde sah sich gezwungen, das verlangte Lösegeld zu zahlen.

03.03.2016- spiegel.de

Über drei Milliarden Accounts gekapert

28.10.2016 – heise.de

Rekord-DDoS-Attacke mit 1,1 Terabit pro Sekunde gesichtet

9.09.2016 –heise.de

Sie lieben Social Media? Hacker auch.

28.09.2016 – TÜV Rheinland

Dateilose Infektion: Einbruch ohne Spuren

13.02.2017 – heise.de

Riesiges Necurs-Botnetz wird nun anscheinend zur Aktienmanipulation eingesetzt

21.03.2017 – heise.de


Szenario	Schadsoftware	Preisgabe von Informationen	Physische Einwirkungen
Schlagworte	Malware, Virus, Wurm, Phishing, Spoofing	Social Engineering, Spyware/ Keylogger (Sniffing)	Diebstahl, Einbruch, Umwelteinflüsse
Kennzeichen	Verbreitung durch: E-Mail, Kurznachrichten am Mobiltelefon, Webseiten, USB-Sticks, …	Methode: Ausnutzen von Vertrauen, Hilfsbereitschaft, Angst, Respekt, …	Ziel: Hardware, Netzwerkzugriff, Dokumente, …
Auswirkung	• Datenverlust • Erpressung • Abschalten des IT-Systems: dringende Aufgaben können nicht erledigt werden • Vertrauen der Bürger/Kunden verringert sich	• Diebstahl der digitalen Identität (Passwörter, Nutzernamen) • Abfluss von Informationen • Sicherheit von Behördengeheimnissen ist nicht länger gewährleistet	• Datenverlust • Unberechtigter Zugang zu IT-System • Ausfall der IT-Systeme durch Diebstahl • Installation von Schadsoftware • Informations-sicherheit ist nicht länger gewährleistet


RECHTLICHE RAHMENBEDINGUNGEN

Wir haben es mit einem „Universum“ an Gesetzen, Vorschriften, Regelungen und Verpflichtungen zu tun

- IT-Sicherheitsgesetz
- BDSG
- Datenschutzgesetz der Länder
- Verträge
- Versicherungen
- Europäische Datenschutz Grundverordnung (25. Mai 2018)
- Bayerisches eGovernment-Gesetz
- …


BEISPIEL: EU DATENSCHUTZ GRUNDVERORDNUNG

Art. 32
„... geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“

- Bußgeld von bis zu 2%/10 Mio. EUR bis 4%/20 Mio. EUR, bezogen auf den weltweit erzielten Jahresumsatz des Unternehmens, je nachdem welcher der Beträge höher ist. (Art. 83)

Spätestens bis Mai 2018 braucht jedes Unternehmen ein Datenschutz- und IT-Sicherheitskonzept!

ISIS 12
Informationssicherheit für den Mittelstand


ISMS

ISIS 12
Informationssicherheit
für den Mittelstand


ISIS12 - HINTERGRUND

- Gründung des Netzwerkes „Informationssicherheit für den Mittelstand“ innerhalb des Clusters
- Ziel: Entwicklung eines einfachen Vorgehensmodell zur Einführung von Informationssicherheit
- Zunächst für KMU


ISIS12 – WAS IST NEU?

- Verständlich beschriebener 12-stufiger Prozess, der den Einstieg ins ISMS erleichtert (ISIS12-Handbuch)
- Integration ISMS mit IT-Service Management (IT-SM)
- Spezifischer ISIS12-Maßnahmensatz (ISIS12-Katalog)
- 12-stufiger Prozess wird als Workflow abgebildet


ISIS12 – **I**nformations-**SI**cherheitsmanagement**S**ystem in **12** Schritten

ISIS12

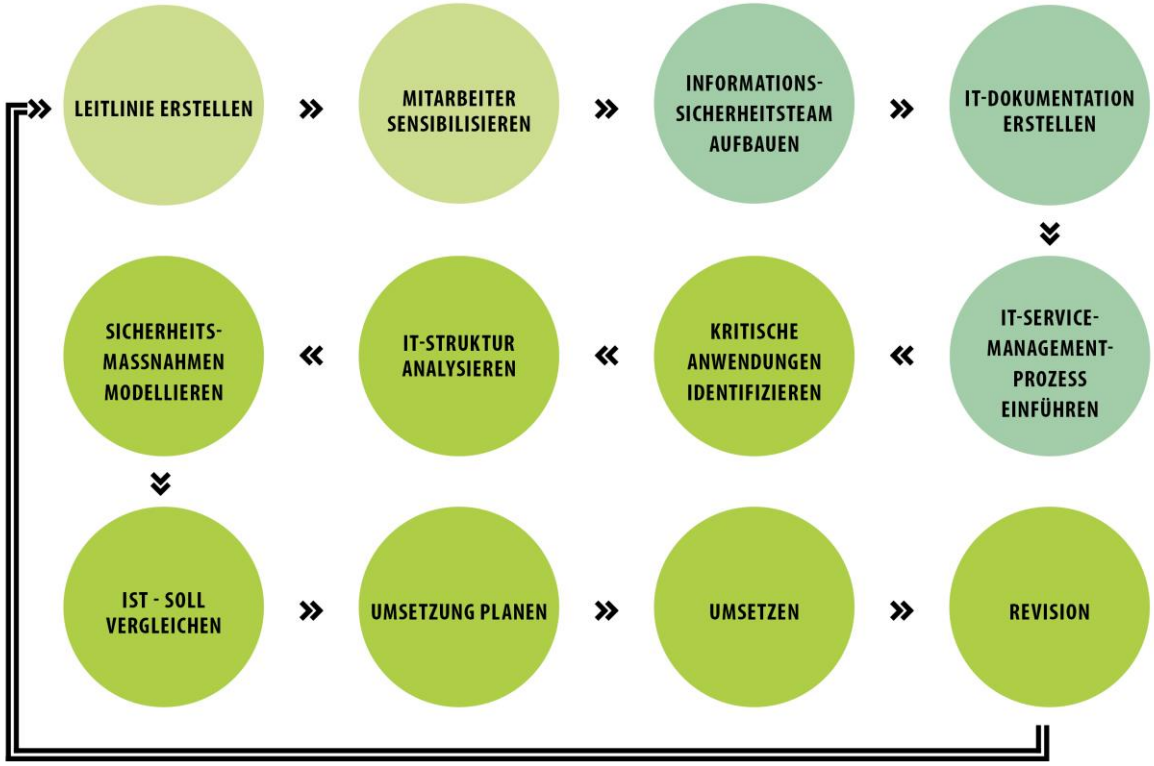
- ist ein Verfahren zur Einführung und Verbesserung der Informationssicherheit in mittelständischen Unternehmen und Organisationen
- gilt als Vorstufe zum BSI IT-Grundschutz-Zertifikat
- Handbuch und Katalog können über das Cluster bezogen werden
- Einführung kann durch zertifizierte ISIS12-Dienstleister begleitet werden
- Workflow wird durch ein vom Netzwerk entwickeltes Softwaretool dargestellt

INFORMATIONSSICHERHEIT IN 12 SCHRITTEN

Initialisierungsphase
Schritte 1-2

Aufbau- und
Ablauforganisation
Schritte 3-5

Entwicklung und
Umsetzung ISIS12
Konzept
Schritte 6-12



ISIS 12
Informationssicherheit für den Mittelstand


ISIS12 – FAKTEN (I)

	ISO/IEC 27001:2013	BSI-Grundschutz (auf Basis ISO/IEC 27001)	ISIS12
Grad der technischen Detaillierung	Schreibt keine technischen Umsetzungsdetails vor; Maßnahmenziele und Maßnahmen gelten nicht mehr (seit 2013) verpflichtend; risikoorientierter Ansatz	Technisch sehr detailliert, konkret und umfangreich	Konkrete Handlungs-empfehlungen, stark geführt, basiert auf dem IT-Grundschutz-Vorgehensweise und -Katalogen
Zertifizierungs-aufwand	Aufwand wird nach ISO 27006 kalkuliert und ist abhängig von Mitarbeiteranzahl des Geltungsbereich; beginnt bei 5 PT für Erst-Audit	Aufwand mind. 15 PT unabhängig vom Geltungsbereich	Erst-Zertifizierungs-Audit dauert i.d.R. 2 PT und Überwachungs-Audit - 1 PT
Zertifizierungs-stellen	Zehn akkreditierte Zertifizierungsstellen	BSI	DQS GmbH
Verbindung mit Risikomana-gement	Freie Wahl einer angemessenen Risikomethodik (vgl. z.B. ISO 27005), Fokus auf die Risiken	Sollte mit der Risikoanalyse 100-3 des BSI einhergehen, andere zulässig	Immanente Risikoanalyse, bei einem höheren Schutzbedarf wird eine Risikoanalyse nach BSI-Standard 100-3 empfohlen

Quelle: Gutachten zur Anwendbarkeit von ISIS12 in der öffentlichen Verwaltung; Fraunhofer AISEC; November 2014


ISIS12 – FAKTEN (II)

	ISO/IEC 27001:2013	BSI-Grundschutz (auf Basis ISO/IEC 27001)	ISIS12
Werkzeuge zur Unterstützung	Verschiede Tools Verfügbar. Anwendung und Zertifizierung auch ohne Tools möglich.	Mehrere (auch kostenfreie) Tools am Markt verfügbar. Das BSI hat ein eigenes Tool. Tooleinsatz wird dringend empfohlen.	ISIS12-Software und kommerzielles Tool stehen zur Verfügung. Einsatz des Tools wird empfohlen.
Voraussetzung für Zertifizierung	Das ISMS sollte mindestens bereits 6 Monate betrieben werden.	Das ISMS sollte mindestens bereits 6 Monate betrieben werden.	Die 12 Schritte des ISMS müssen einmal komplett durchlaufen und wirksam umgesetzt worden sein.
Kombination mit anderen Zertifikaten	Zertifizierung ist kombinierbar, z.B. mit ISO 9001 (im Kombi-Audit ca. 30% weniger Aufwand)	Die Kombination mit einer anderen Zertifizierung ist beim BSI nicht möglich	Kombinierbar mit ISO 9000 (Qualitätsmanagement) und ISO 14000 (Umweltmanagement) und ISO 20000 (IT-Servicemanagement)

Quelle: Gutachten zur Anwendbarkeit von ISIS12 in der öffentlichen Verwaltung; Fraunhofer AISEC; November 2014

ISIS 12
Informationssicherheit für den Mittelstand


ZERTIFIZIERUNG NACH ISIS12

- Möglichkeit zur Zertifizierung durch die DQS GmbH
- Zertifikatsgültigkeit von 3 Jahren, inkl. 2 Überwachungsaudits
- Auditierung durch zertifizierte ISIS12-Auditoren
- Unterstützung durch ISIS12-Dienstleister möglich

ISIS 12
Informationssicherheit für den Mittelstand


VORGEHENSWEISE ISIS12-BERATUNGSPROJEKT

1. Kontaktaufnahme mit einen ISIS12-Dienstleister
2. Gemeinsames Festlegen der Arbeitsaufteilung der ISIS12-Arbeitspakete zwischen Unternehmen/Organisation und zertifizierten ISIS12-Dienstleister
3. Aufwandsschätzung mit Angebot
4. Vereinbarung von Projektmeilensteinen
5. Nennung der Verantwortlichen
6. Vertragsabschluss und Umsetzung
7. Zertifizierung (optional)


FÖRDERMÖGLICHKEIT - DIGITALBONUS

Fördergegenstand beim Digitalbonus sind Maßnahmen aus den Bereichen:

- Entwicklung, Einführung oder Verbesserung von Produkten, Dienstleistungen und Prozessen durch IKT-Hardware, IKT-Software sowie Migration und Portierung von IKT-Systemen und IKT-Anwendungen im Unternehmen

- Einführung oder Verbesserung von IT-Sicherheit im Unternehmen.

Der **Digitalbonus** wird in drei Varianten (Standard, Plus und Kredit) zur Verfügung stehen.


FÖRDERMÖGLICHKEIT - DIGITALBONUS

- Zuwendungsempfänger

	Kleine	Mittlere
Mitarbeiter	< 50	< 250
Jahresumsatz	≤ 10 Mio. Euro	≤ 50 Mio. Euro
Bilanzsumme	≤ 10 Mio. Euro	≤ 43 Mio. Euro

ISIS 12
Informationssicherheit für den Mittelstand


FÖRDERMÖGLICHKEIT - DIGITALBONUS

- Höhe der Förderung

Bis zu	**Digitalbonus Standard**
10.000 €	Zuschuss für Digitalisierungsmaßnahmen und IT-Sicherheit
Oder	
Bis zu	**Digitalbonus Plus**
50.000 €	Zuschuss für Digitalisierungsmaßnahmen mit besonderem Innovationsgehalt
Oder/und	
Bis zu	**Digital Kredit**
2 Mio. €	Zinsverbilligtes Darlehen zusätzlich oder alternativ zu den Digitalbonus-Zuschüssen

ISIS 12
Informationssicherheit für den Mittelstand


FÖRDERMÖGLICHKEIT - DIGITALBONUS

1. Antrag
2. Prüfung
3. Förderbescheid
4. Projektdurchführung
5. Verwendungsnachweis
6. Auszahlung

Weitere Informationen unter **www.digitalbonus.bayern**


FÖRDERPROGRAMM FÜR KOMMUNEN IN BAYERN

Art und Umfang der Zuwendung:

- 50 % der Kosten für Beratung, Dienstleistung und Zertifizierung werden finanziell gefördert; der Höchstbetrag der Förderung ist jedoch auf max. 15.000 € begrenzt
- Förderung von Beratungsleistungen ist auf max. 1200 € (brutto) je Beratertag beschränkt
- Mind. zuwendungsfähige Kosten in Höhe von 2.500 € (Bagatellgrenze)


ISA+ INFORMATIONS-SICHERHEITS-ANALYSE

Bedarfsanalyse der Informationssicherheit

- Fragenkatalog umfasst 50 Fragen
- Behandelt die Themengebiete:
  - Technik (u.a. zu vorhandenen IT-Systemen, Datensicherung, Notfallvorsorge)
  - Organisation (u.a. zu Richtlinien, Anweisungen, Schulung und Verantwortlichkeit…)
  - Recht (u.a. zu Compliance und Leistungen Dritter…)
  - Allgemeines (u.a. Unternehmensgröße…)
- Antwortmöglichkeiten nach Reifegradmodell

ISA+ Informations-Sicherheits-Analyse


ISA+ INFORMATIONS-SICHERHEITS-ANALYSE

- Softwareunterstützung ist möglich
- Unterstützung zur Ermittlung des Reifegrades durch ausgebildete Berater
- Öffentlicher Fragenkatalog verfügbar über den Bayerischen IT-Sicherheitscluster e.V.
- Zusatzmodul „Einstieg in die Produktion“


BAYERISCHER IT-SICHERHEITSCLUSTER E.V.

Gründung:

- 2006 als Netzwerk (Cluster) in Regensburg
- 2012 Eröffnung der Geschäftsstelle Augsburg
- 2013 Überführung in einen Verein

Mitglieder:

- Unternehmen der IT-Wirtschaft
- Unternehmen, die Sicherheitstechnologien nutzen
- Hochschulen, Weiterbildungseinrichtungen
- Juristen

SILVER Cluster Management Excellence
DEDICATED TO CLUSTER EXCELLENCE

ITSECURITY
Bavarian IT Security & Safety Cluster


Das Bayerische IT-Sicherheitscluster

ÖFFENTLICHKEITSARBEIT / KOOPERATIONSPROJEKTE

SECURITY

- Datenschutz
- Cloud Security
- Industrial IT Security
- Sicheres Smart Grid
- Cybersicherheit
- Informationssicherheitsmanagement

SAFETY

- Automotive Safety
- Safety Standards
- Methoden der funktionalen Sicherheit
- Eingebettete Systeme

14
Hochschulen, Forschungs- und Weiterbildungsinstitute

102
Unternehmen

Stand 06.10.2016


VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Kontakt:

Felix Struve
Bayerischer IT-Sicherheitscluster e.V.
Franz-Mayer-Str. 1
93053 Regensburg
Tel.: 0941/604 88 9 15
Mail: felix.struve@it-sec-cluster.de

Unterstützt durch das
Bayerische Staatsministerium des Innern, für Bau und Verkehr
Initiative Cybersicherheit Bayern
ISIS 12
Informationssicherheit für den Mittelstand