5. Kommunaler IT-Sicherheitskongress 2018

Aus der Praxis für die Praxis

„SiKoSH leuchtet ein“

SICHER

EFFEKTIV

GEMEINSAM

SiKoSH
SICHERHEIT FÜR KOMMUNEN
IN SCHLESWIG-HOLSTEIN

SiKoSH – wie alles begann

- Ziel laut Projekthandbuch: Kommunal angemessenes Sicherheitsniveau orientiert am BSI-Grundschutz
  - Unterstützung beim Aufbau ISMS inkl. Sicherheitskonzept
  - Nachhaltigkeit sichern
- Projektgruppe
  - Kommunen
  - Prüfbehörden (ULD und LRH)
  - Partner (FHH, ISK.RLP)
  - ZIT (Zentrales IT-Management des Landes Schleswig-Holstein)
  - Sicherheitsmanagement Dataport + André Glenzer (www.andreglenzer.com) - Beratung und Konzepterstellung -
  - Dr. Werner Degenhardt – Psychologie der Informationssicherheit - Marketing und Mitarbeitersensibilisierung -
  - KomFIT

SiKoSH
SICHERHEIT FÜR KOMMUNEN IN SCHLESWIG-HOLSTEIN

tandard heute

aches Einstiegsframework
iell für kommunale Anwender
vickelt.

t in Konkurrenz zu etablierten
rmationssicherheitsframeworks,
z.B. IT-Grundschutz, ISIS12 oder
01, sondern als Ergänzung und
tieg zu diesen zu verstehen.

utert die Umsetzungsphasen und
renziert auf Begleitdokumente
chbuch“)

SiKoSH Standard - Vorgehensweise zur Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach SiKoSH

Version:	1.0.0
Datum:	02.11.2017
Kontakt:	KomFIT e.V. Kiel sikosh@komfit.de https://www.sikosh.de

Temporäre Informationssicherheitsorganisation

initiiert

ISMS	•Aufbau- und Ablauforganisation – Leitlinien	Quickcheck 1 (QC 1)
Anwareness	•Sensibilisierung – Schulung	QC 2
Standards	•Übergreifende Aspekte (Freigaben, Malware, etc.)	QC 3
Allgemein	•Gebäude – Einkauf und Entsorgung - Auftrags-DV	QC 5 - 7
Technik	•Systeme, Verzeichnisdienst, E-Mail	QC 8 - 11
Verfahren	•Rollen und Rechte	QC 12
Notfall	•Notfallkonzept	QC 13

Querschnittsprüfung QC 14

Sicherheitskonzept

SiKoSH – Phase 1 - ISMS

Temporäre Organisation	Bestandsaufnahme	Grundlagen schaffen	ISMS Organisationsstruktur aufbauen	Erste Umsetzungsschritte
Behördenleiter, IT-Leiter, bDSB, Personalrat …	• Leitlinie vorhanden • ISB bestellt? • Prozesse geregelt? 📖 Quickcheck 1	• Behördenleiter einbinden • Leitlinie erstellen 📖Handreichung für Behördenleiter 📖Muster Informationssicher-heitsleitlinie	• Rollen besetzen • Aufgaben abgrenzen 📖Bestellung ISB 📖Schulung ISB 📖Muster-Leitlinie ISMS / DSMS	Empfehlung: Awareness • Quickcheck 2 • Sensibilisierungskampagne

Temporäre Informationssicherheitsorganisation

initiiert

ISMS	•Aufbau- und Ablauforganisation – Leitlinien	Quickcheck 1 (QC 1)
Anwareness	•Sensibilisierung – Schulung	QC 2
Standards	•Übergreifende Aspekte (Freigaben, Malware, etc.)	QC 3
Allgemein	•Gebäude – Einkauf und Entsorgung - Auftrags-DV	QC 5 - 7
Technik	•Systeme, Verzeichnisdienst, E-Mail	QC 8 - 11
Verfahren	•Rollen und Rechte	QC 12
Notfall	•Notfallkonzept	QC 13

Querschnittsprüfung QC 14

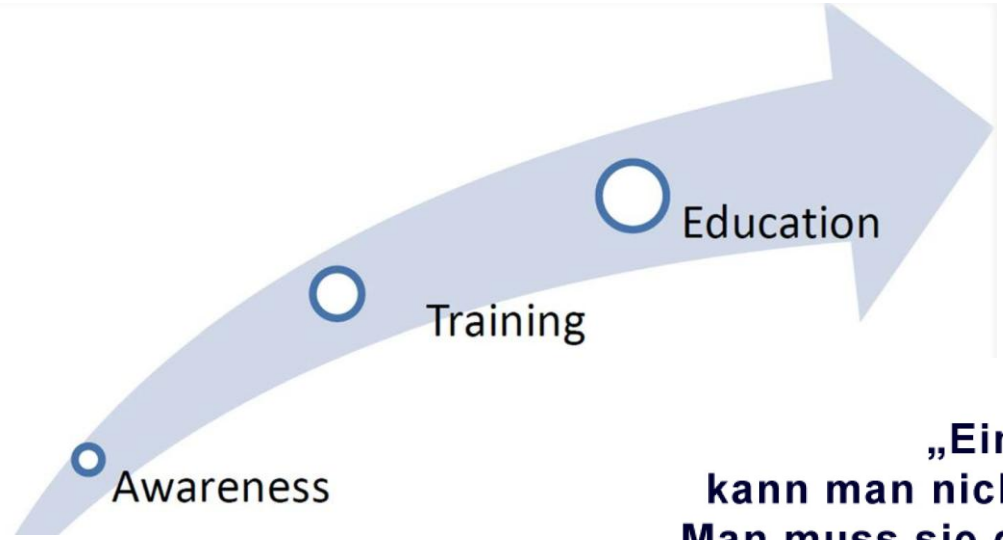
Sicherheitskonzept

SiKoSH-Beispiel Sensibilisierung

ner Degenhardt, LMU München

Version:	1.0.0 Dr. Werner Degenhardt, München Frank Weidemann, Kiel
Datum:	02.11.2017
Kontakt:	KomFIT e.V. Kiel sikosh@komfit.de https://www.sikosh.de werner.degenhardt@codeandconcept.de, degenhardt@lmu.de http://www.codeandconcept.de

Kann man besseres Sicherheitsverhalten lernen?



Enisa "The new user's guide: How to raise information security awareness"

„Eine Angewohnheit kann man nicht aus dem Fenster werfen. Man muss sie die Treppe hinunter prügeln. Stufe für Stufe.“

– Mark Twain

Phishing-Training bei der Landeshauptstadt Kiel

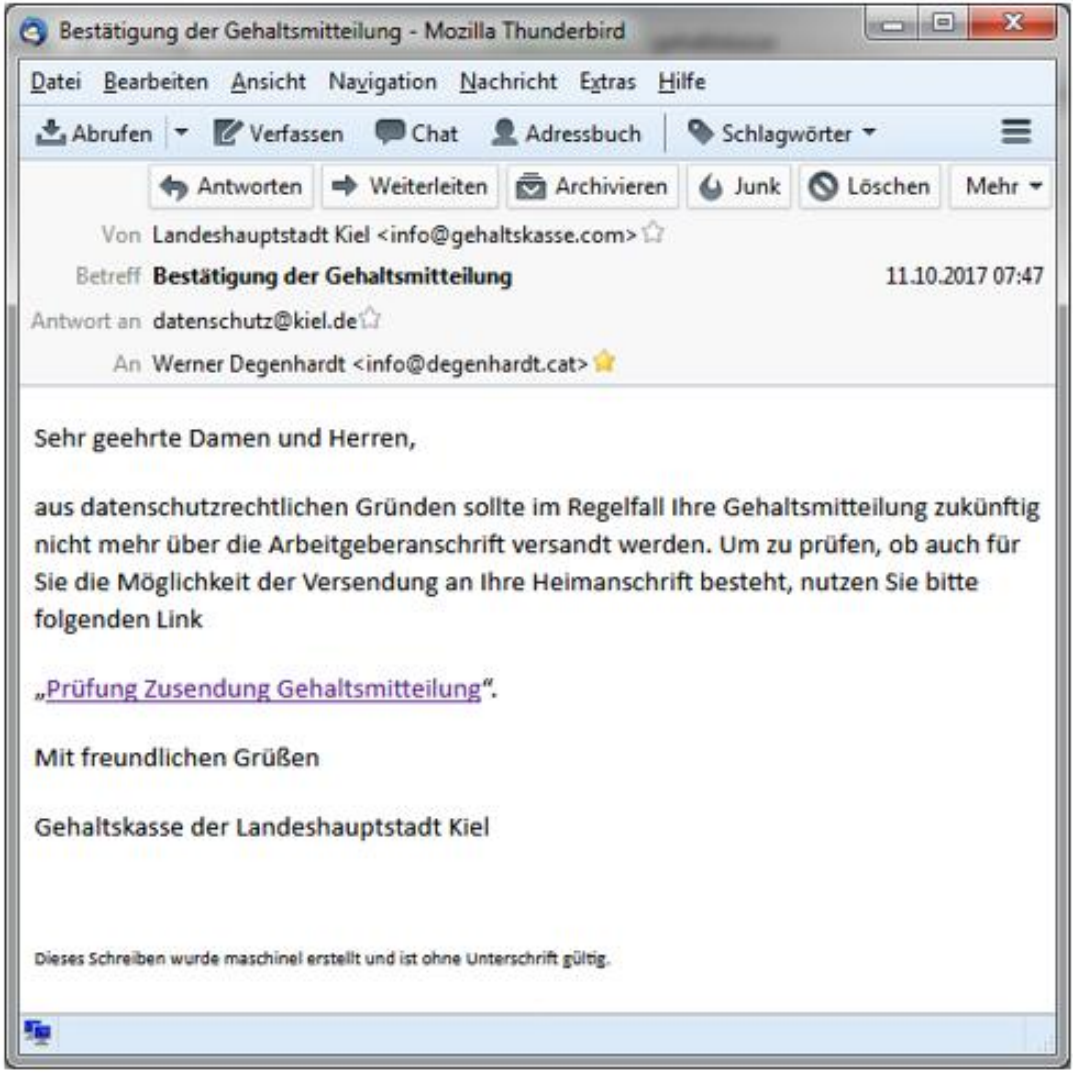
02.11.2017 KomFIT 2017

OB Dr. Ulf Kämpfer auf der KomFIT 2017 (sinngemäß): „Meine größten Sorgen morgens nach dem Aufwachen sind Feuer, Terrorismus und Datenverlust. Ich warte nur darauf, dass der erste Bürgermeister nach einem massiven Datenverlust zurücktreten muss.“

Phishing-Training bei der Landeshauptstadt Kiel

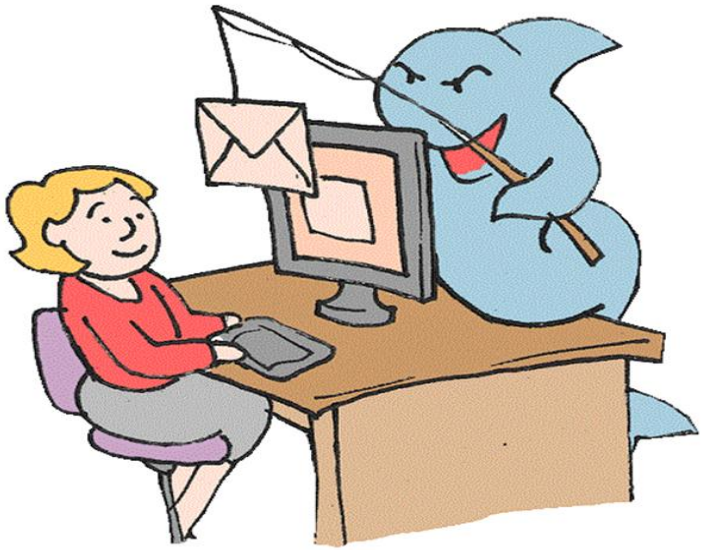
Grobe Planung	• Rechtfertigung, Umsetzung, Aufwand
Stakeholder einbinden	• Oberbürgermeister, Datenschützer, IT-Leiter, Personalrat, Gleichstellungsbeauftragte, Vertrauensmann Schwerbehinderte
Design	• Mailentwürfe, Technische Realisierung, Umsetzung, begleitende Maßnahmen
Phase 1	• Angriff
Ergebnisse	• Auswertung, Abstimmung mit Stakeholdern, Konzept überarbeiten, nächste Phase planen
Phase x	

Phishing-Training Welle 1
- Böse Mail mit Link -



Sie wurden gefischt!

Kiel. Sailing.City.



Die E-Mail, die Sie erhalten haben und die Sie auf diese Seite gebracht hat, imitiert eine Phishing-E-Mail. Es ist eine Phishing-Simulation.

Phishing-E-Mails verschleiern ihre Herkunft und sollen Sie dazu bringen, auf bösartige Links zu klicken.
Sie haben diese Phishing-Simulation bekommen, um zu zeigen, wie ein Phishing-Betrug tatsächlich durchgeführt wird und wie einfach es ist, von diesen cleveren Betrügereien getäuscht zu werden.

Aber keine Sorge! Dies ist keine Prüfung oder dergleichen. Auch Ihre Daten werden nicht gespeichert.

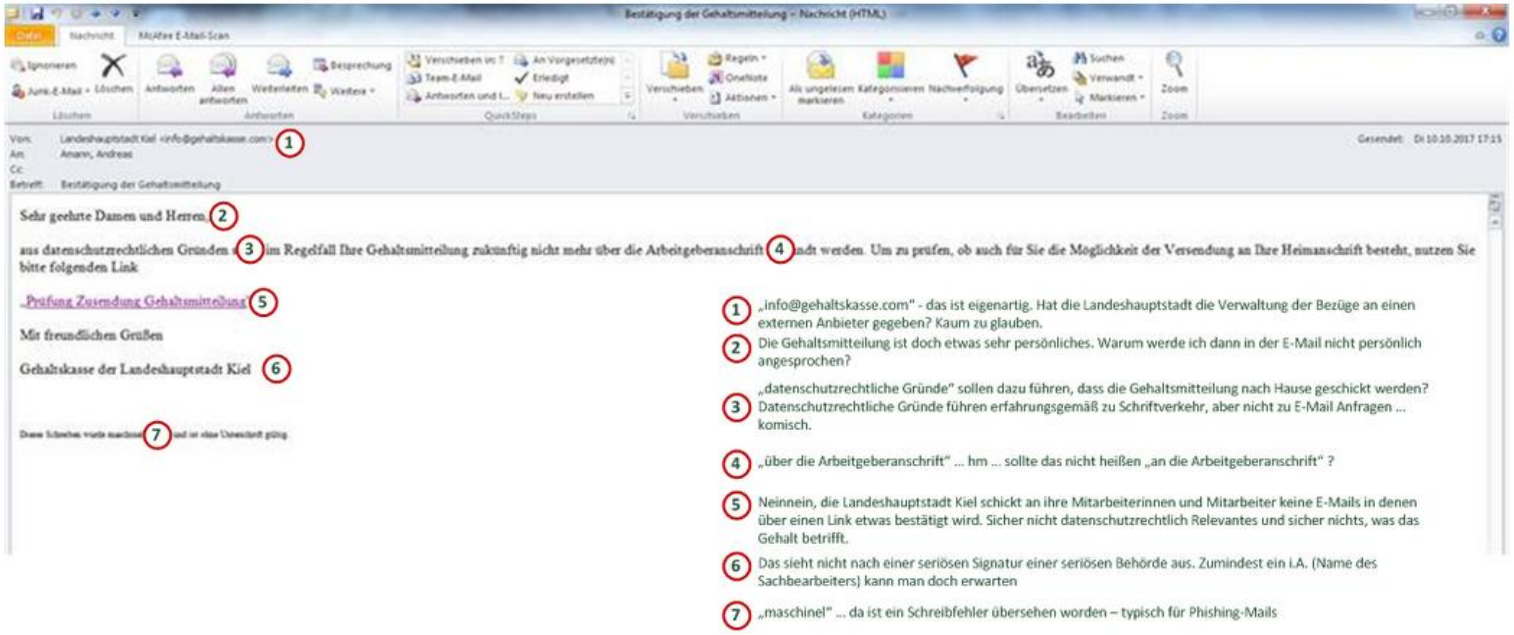
Was wäre passiert, wenn dies ein echte Phishing-Mail gewesen wäre, wenn es sich um einen echten Phishing-Betrug gehandelt hätte? Dann hätten Betrüger Ihren Computer mit einem Trojaner infizieren können, indem Sie einfach auf den Link in der E-Mail klicken. Oder, wenn Sie Ihren Benutzernamen und Kennwort oder andere sensible Informationen zur Verfügung gestellt hätten, könnte sogar Schlimmeres passieren. Stellen Sie sich vor, was diese Person mit den von Ihnen gestohlenen Informationen alles anfangen könnte? Im Prinzip reicht ein infizierter Rechner, um das gesamte Netzwerk der Landeshauptstadt Kiel in Schwierigkeiten zu bringen oder ganz lahm zu legen.

Aber, wie gesagt, das war keine echte Phishing-Mail, sondern ganz im Gegenteil: wir möchten Ihnen helfen, nicht noch einmal auf diesen Trick hereinzufallen.

Sie sehen unten ein Bildschirmfoto dieser E-Mail mit Hinweisen auf Merkmale, die Misstrauen erregen könnten und sollten.

Außerdem finden Sie am Ende dieser Seite einen Link zum Behörden-IT-Sicherheitstraining der Landeshauptstadt Kiel, das Ihnen helfen soll, diese bösartigen Mails zu erkennen und Ihre Daten zu schützen. Die Teilnahme ist freiwillig und zu jeder Zeit möglich. Informationen über Teilnahme oder gar Erfolg des Trainings werden nicht erfasst, personenbezogene Auswertungen finden nicht statt.

Wie erkenne ich eine Phishing-Mail?



1. „info@gehaltskasse.com" - das ist eigenartig. Hat die Landeshauptstadt die Verwaltung der Bezüge an einen externen Anbieter gegeben? Kaum zu glauben.
2. Die Gehaltsmitteilung ist doch etwas sehr persönliches. Warum werde ich dann in der E-Mail nicht persönlich angesprochen?
3. „datenschutzrechtliche Gründe" sollen dazu führen, dass die Gehaltsmitteilung nach Hause geschickt werden? Datenschutzrechtliche Gründe führen erfahrungsgemäß zu Schriftverkehr, aber nicht zu E-Mail Anfragen ... komisch.
4. „über die Arbeitgeberanschrift" ... hm ... sollte das nicht heißen „an die Arbeitgeberanschrift" ?
5. Neinnein, die Landeshauptstadt Kiel schickt an ihre Mitarbeiterinnen und Mitarbeiter keine E-Mails in denen über einen Link etwas bestätigt wird. Sicher nicht datenschutzrechtlich Relevantes und sicher nichts, was das Gehalt betrifft.
6. Das sieht nicht nach einer seriösen Signatur einer seriösen Behörde aus. Zumindest ein i.A. (Name des Sachbearbeiters) kann man doch erwarten
7. „maschinel" ... da ist ein Schreibfehler übersehen worden – typisch für Phishing-Mails

Aber Achtung! Nicht immer ist es so einfach zu erkennen. Dies ist nur ein Beispiel.

Für das Behörden-IT-Sicherheitstraining hier klicken!

Wenn Sie das für einen neuen Trick halten, dann ist das gut. Man sollte immer wissen, worauf ein Link verweist und der URL hinter dem Link vertrauen können, bevor man klickt.
Für den Fall gesteigerten Misstrauens haben wir hier einen Link auf das Behörden-IT-Sicherheitstraining im Intranet der Landeshauptstadt Kiel:

http://bits.kiel.de/bits/bits/index.html

Kopieren Sie einfach den Link in die Adresszeile Ihres Browsers und Sie können mit den Lerneinheiten im BITS (Behörden-IT-Sicherheitstraining) beginnen.

Erfahrungen

- Die Klickquote liegt bei 28%
- Die meisten Benutzer reagieren positiv auf die Kampagne

Phishing-Training Welle2 18.11.2017 - Böse Mail mit Anlage -

Sehr geehrter Herr xxx,

auf dem Rathausplatz, dem Holstenplatz, dem Asmus-Bremer-Platz und der Altstadt wurde in diesem Jahr unter maßgeblicher Beteiligung der Kieler Stadtverwaltung eine – wie die Kieler Nachrichten es nannten – „Revolution auf dem Weihnachtsmarkt“ umgesetzt. Was Sie in diesem Jahr auf den Kieler Weihnachtsmärkten zu sehen bekommen, gab es in den 45 Jahren seit Gründung der adventlichen Budenstadt noch nie. Wir möchten uns auf diesem Wege ganz herzlich bei allen Beschäftigten der Verwaltung für Ihre Arbeit im jetzt bald vergangenen Jahr bedanken.

Wir freuen uns, Ihnen als vorweihnachtliches Dankeschön einen Gutschein für einen kostenfreien Glühwein (mit oder ohne Alkohol) und eine kostenfreie Bratwurst anbieten zu können!

Um den Vorteil nutzen zu können, drucken Sie einfach die in der Anlage beigefügten Gutscheine aus und legen diese an einem der vielen Stände der Kieler Weihnachtsmärkte vor. Bitte beachten Sie aber, dass die Gutscheine nur bis zum 22.12.2017 gültig sind.

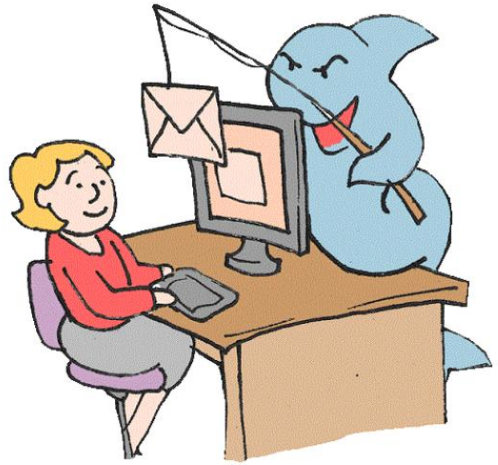
Wir wünschen Ihnen und Ihrer Begleitung viel Spaß und gute Unterhaltung auf den Kieler Weihnachtsmärkten.

Mit freundlichen Grüßen

Ihr Christmas-Event-Management-Team (CEMT)

Phishing-Training Welle 2 bei der Stadt Kiel

Phishing-Training Welle 2 bei der Stadt Kiel



Oha! Wie konnte das passieren?

Sie haben:
einer unbekannten Website vertraut und zugelassen, dass dieses .pdf-Dokument ein Programm auf Ihrem Rechner ausführt.

Dieses Programm hätte ein Trojaner sein können, der ihren Daten, ihren Dokumenten, ihren Bildern und – wenn es dumm läuft – dem ganzen Netzwerk der Landeshauptstadt schweren Schaden zufügt.

Faustregel:

Wenn man eine Sicherheitswarnung beim Öffnen eines Anhangs bekommt und nicht weiß, welche Folgen es hat, wenn man die Datei trotzdem öffnet:

Den IT Service (unter helpdesk@kiel.de oder Telefon 4444) fragen, bevor Sie die Datei öffnen

Tatsächlich gibt es viele Hinweise, die es den Mitarbeiterinnen und Mitarbeitern der Landeshauptstadt ermöglichen, zwischen „guten“ und „bösen“ Email-Anhängen zu unterscheiden.

Das Sicherheitstraining im Intranet der Landeshauptstadt Kiel zeigt Ihnen, wie Sie Schaden von sich und anderen fernhalten.

http://bits.kiel.de/bits/bits/index.html

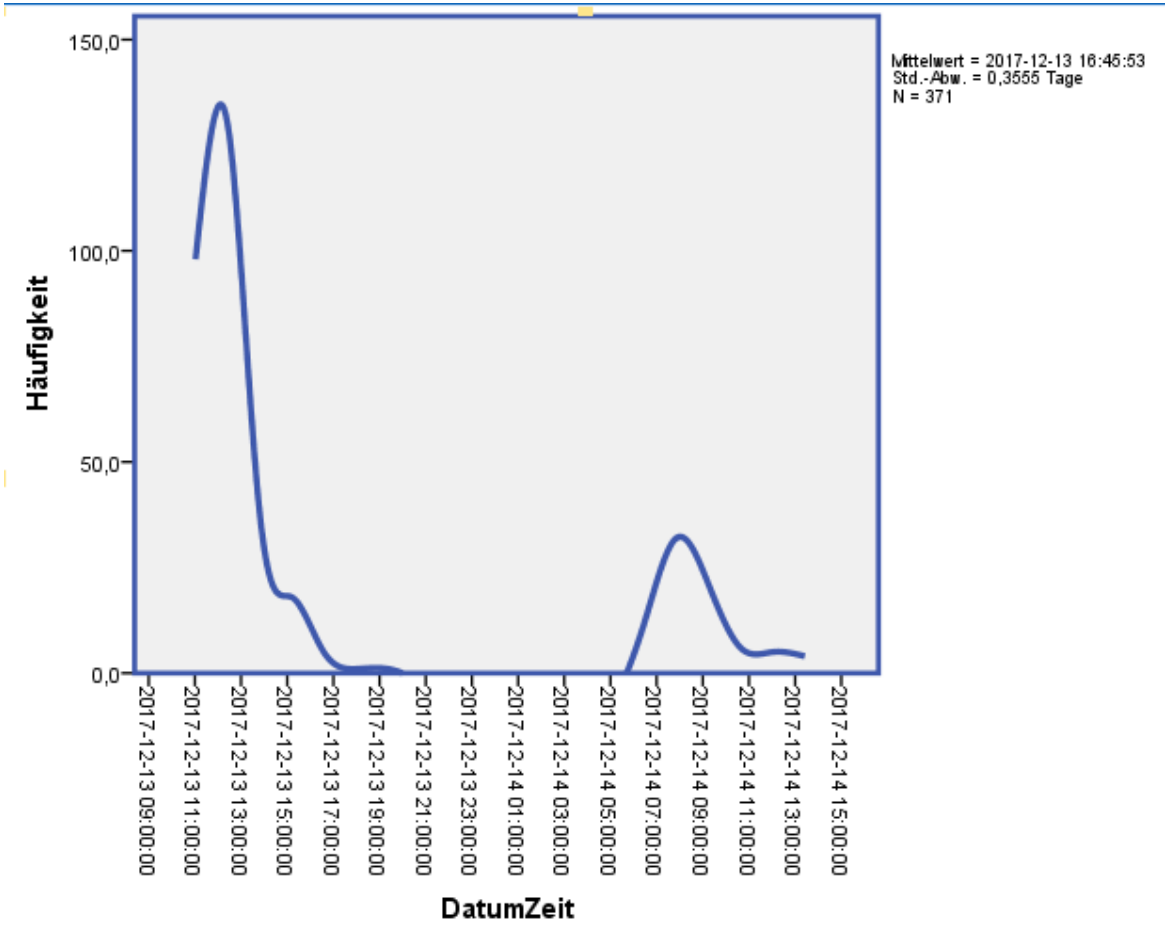
Kopieren Sie einfach den Link in die Adresszeile Ihres Browsers und Sie können mit den Lerneinheiten im BITS (Behörden-IT-Sicherheitstraining) beginnen.

Erfahrungen

- Es gab nur wenig negative Reaktionen (und auch die waren eigentlich positiv*)
  - Danke, eine sehr gute Idee und sehr lehrreich!!
  - CEMT überprüft . . . netter Versuch HA HA HA oder besser gesagt HO HO HO
  - Ich war an dem Gutschein gar nicht so interessiert, aber sehr neugierig, wer denn hier lobt (das passiert bei der Stadt ja eher selten), und ich vertraue auch unterbewusst auf die städt. Abwehrmaßnahmen (zuhause hätte ich keinen Gutschein aufgemacht, weil ich weiß, dass mir niemand etwas schenken will). Eine gute Aktion!!!
  - Wir Mitarbeiter/innen sind uns weitestgehend einig, dass diese Phishing Mails überhaupt nicht sinnvoll sondern nur ärgerlich sind. Sie sensibilisieren nur insofern, als dass “echte“ und rechtsverbindliche Anhänge nicht mehr geöffnet werden. Es würde mehr Sinn machen, endlich ein effektives Schutzprogramm zu kaufen oder mit einem gewissen Risiko zu leben. Ansonsten wird die Stadtverwaltung nicht von Trojanern und Viren lahmgelegt sondern von völlig verunsicherten Mitarbeitern.

* Warum positiv? - Weil sie der IT zeigen, wie ihre Benutzer wirklich denken und was sie erwarten ... wichtig für das Erwartungsmanagement.

Und die Quote?



Nach etwas mehr als 24 Stunden

13%!!!

Phishing-Training Welle 3

Von: Informations- und Telekommunikationstechnik der Landeshauptstadt Kiel <Jan.Koppelmann@kiel.de> Gesendet: Mo 16.04.
An: Amann, Andreas
Cc:
Betreff: Prüfung Zugangsberechtigung Internet

Sehr geehrter Herr Amann,

die Sicherheitsabteilung der Landeshauptstadt Kiel wird Sie in Bezug auf die Sicherheit der Internetnutzung kontaktieren. Ab dem 01. Mai 2018 werden Veränderungen vorgenommen.

Bitte beachten Sie, dass Ihr Online-Zugang bald abläuft. Um diesen Dienst weiterhin nutzen zu können, klicken Sie bitte auf den untenstehenden Link. Nur so können Sie Ihren Zugang manuell mit unserem Sicherheits-Update aktualisieren:

https://www.klel.de/internetsicherheit

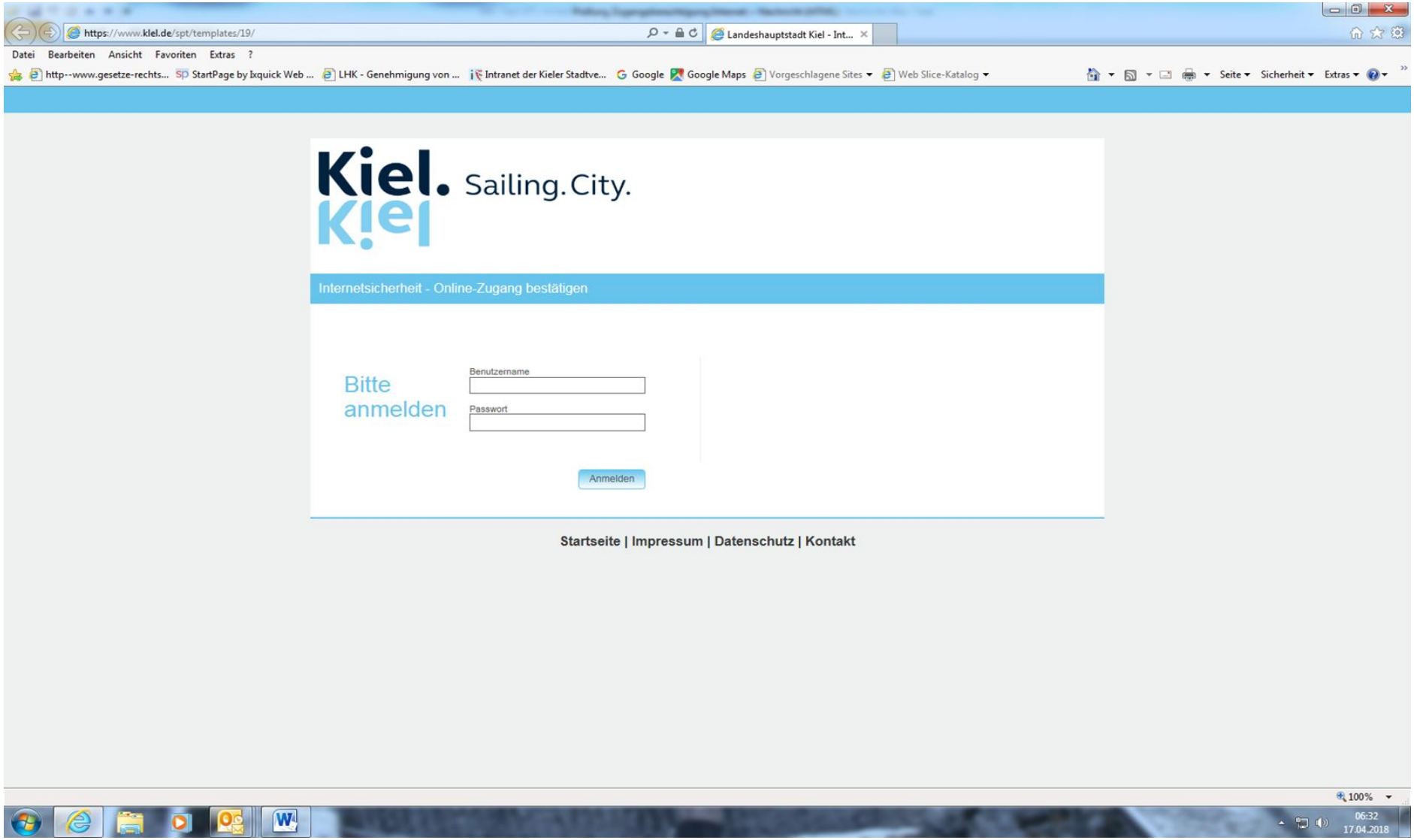
Nach Vervollständigung dieses Schrittes wird sich eine Mitarbeiterin oder ein Mitarbeiter unseres IT-Bereiches mit Ihnen in Verbindung setzen.

Wir entschuldigen uns für die Unannehmlichkeiten.

Mit freundlichen Grüßen

Jan Koppelmann

IT-Leiter – Landeshauptstadt Kiel


https://www.kiel.de/spt/templates/19/
Landeshauptstadt Kiel - Int...
Datei Bearbeiten Ansicht Favoriten Extras ?
Kiel. Sailing.City.
Internetsicherheit - Online-Zugang bestätigen
Bitte anmelden
Benutzername
Passwort
Anmelden
Startseite | Impressum | Datenschutz | Kontakt
100%
06:32
17.04.2018

https://www.kiel.de/spt/education/11/ Sie wurden gephisht!

Datei Bearbeiten Ansicht Favoriten Extras ?

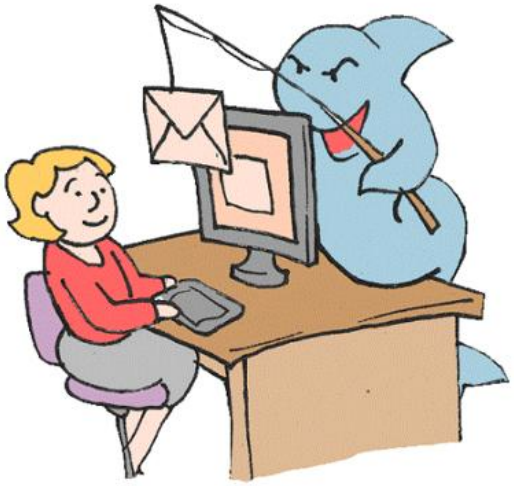
http--www.gesetze-rechts... StartPage by Ixquick Web ... LHK - Genehmigung von ... Intranet der Kieler Stadtve... Google Google Maps Vorgeschlagene Sites Web Slice-Katalog

Seite Sicherheit Extras

Suchen: weitergeleitet Zurück Weiter Optionen

Sie wurden gefischt!

Kiel. Sailing.City.



Oha! Wie konnte das passieren?

Die E-Mail, die Sie erhalten haben und die Sie auf diese Seite gebracht hat, wurde vom Datenschutz- und Datensicherheitsteam der Landeshauptstadt Kiel erstellt und ist Teil einer Sicherheitskampagne.

Wir wollen Ihnen in Ihrem normalen Arbeitsalltag zeigen, wie Internet-Kriminelle vorgehen und wie einfach es sein kann, auf deren Tricks hereinzufallen.

Wenn dies eine echte verbrecherische E-Mail gewesen wäre, dann wären bei vollständigem Ausfüllen des Anmeldeformulars Ihre Zugangsdaten an den Angreifer weiter geleitet worden. Dieser hätte mit Ihren Zugangs all das machen können, das Sie selbst mit Ihren Logindaten in den Systemen der Landeshauptstadt Kiel machen können.

Selbstverständlich erfassen wir nicht, wie Sie auf diese Simulation reagiert haben – und wir haben technisch dafür gesorgt, dass niemand seine kompletten Anmeldedaten in der von uns gestalteten Seite eingeben kann. Denn die Landeshauptstadt wird Sie niemals auffordern, Ihre persönlichen Anmeldedaten preiszugeben! Verraten Sie Ihr Kennwort niemandem, auch keinen Kollegen/Vorgesetzten oder Systemverantwortlichen - schon gar nicht im Internet.

Wenn Sie mehr über unsere Motivation, Sie auf diese Weise sensibilisieren zu wollen, erfahren möchten, finden Sie ergänzende Hinweise im Intranet unter der Rubrik „IT & Telefon“ und dort unter „IT-Sicherheit“ und „IT-Sicherheitstraining BITS“.

Dort finden Sie auch das **Online-Sicherheitstraining „BITS“,** mit dem wir Ihnen die Möglichkeit bieten, auf einfache Weise und zu jeder Zeit zu erfahren, wie Sie sich richtig am Computer und im Internet verhalten. Um direkt zum Sicherheitstraining zu gelangen, klicken Sie hier. Wenn Sie das für einen Trick halten, ist das gut, denn eine Sicherheitsregel lautet, „klicken Sie niemals auf unbekannte Links“.

Alternativ können Sie diesen Link http://bits.kiel.de/bits/bits/index.html in die Adresszeile Ihres Browsers kopieren und sofort mit dem IT-Sicherheitstraining beginnen.

Andreas Amann, App. 901-2771
Jan Koppelmann, App. 901-4074

90%

Reaktionen ☺

- Ist das schon wieder eine hinterhältige, gemeine Falle von Dir? Um uns arme Sachbearbeiter zu verunsichern? Aber so einfach kriegst Du uns nicht… J
- Ist das ein Fake? Unübliche Formatierung der Mail.
- Ich lasse mir doch kein l für ein I vormachen! https://www.klel.de/internetsicherheit Außerdem, was hätte auch der Freischaltungsantrage VOR der Tür zu suchen. Solche Dinge gehören doch ins Intranet. Guter Versuch!
- Nachdem in der Vergangenheit hier hin und wieder „Fake-Mails“ aus der IT rumgingen, um den sicheren Umgang mit dem Internet zu sensibilisieren, bin ich etwas verunsichert, was Ihren angegebenen Link anbetrifft. Ist der Rechtschreibfehler ein Versehen oder beabsichtigt? Bitte um kurze Rückmeldung.

Temporäre Informationssicherheitsorganisation

initiiert

ISMS	•Aufbau- und Ablauforganisation – Leitlinien	Quickcheck 1 (QC 1)
Anwareness	•Sensibilisierung – Schulung	QC 2
Standards	•Übergreifende Aspekte (Freigaben, Malware, etc.)	QC 3
Allgemein	•Gebäude – Einkauf und Entsorgung - Auftrags-DV	QC 5 - 7
Technik	•Systeme, Verzeichnisdienst, E-Mail	QC 8 - 11
Verfahren	•Rollen und Rechte	QC 12
Notfall	•Notfallkonzept	QC 13

Querschnittsprüfung QC 14

Sicherheitskonzept

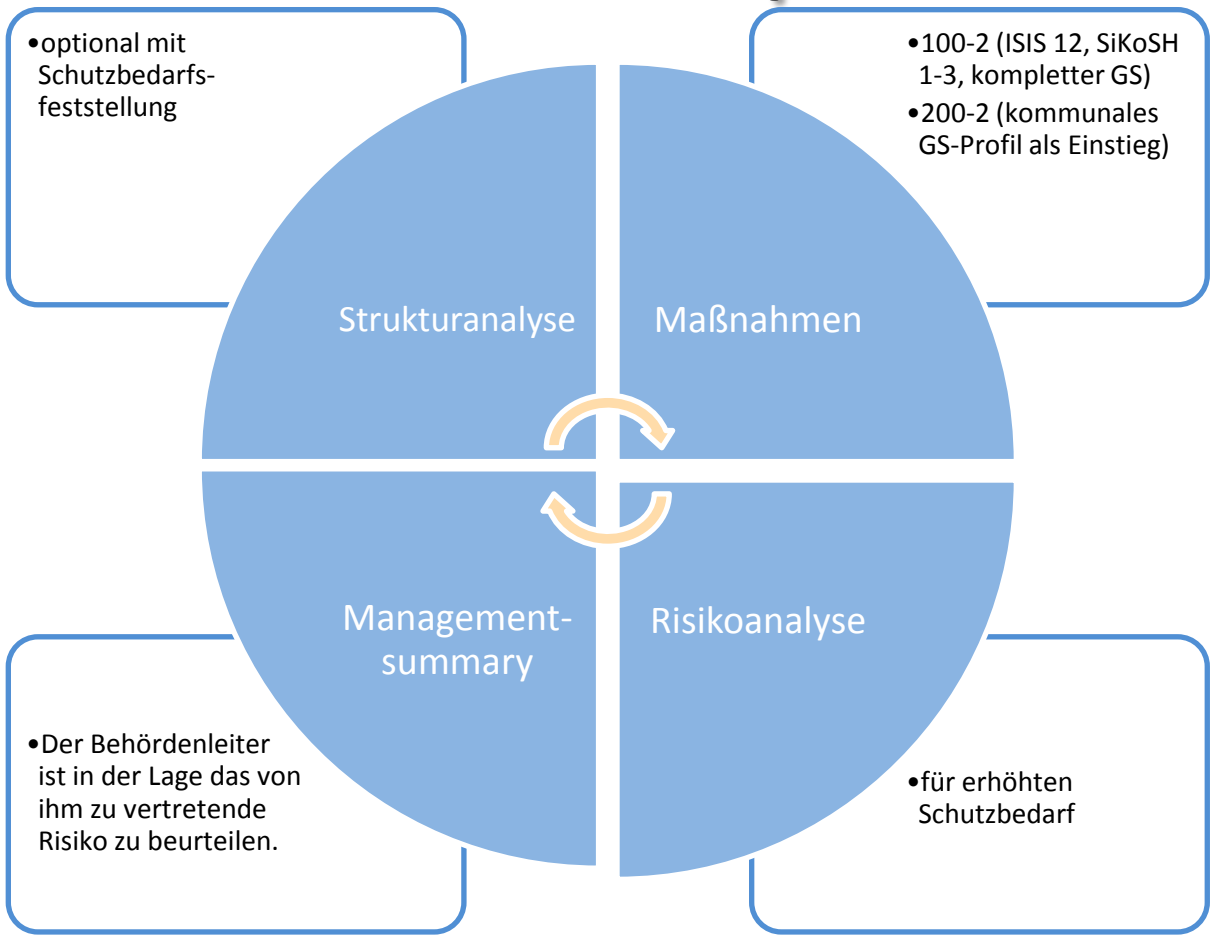
Querschnittsprüfung

- Rudimentäre, kennzahlenbasierte Messung des Erfolgs durch alle Phasen

SiKoSH-Quickcheck Stufe 14: Querschnittsfragen (v. 1.1.0)

Frage	Pun	Prüfpunkte	Priorität	Bewertung	Gewichtete Bewertung	Notizen
1	Ist einem der Institution angemessenes ISMS implementiert und verfügt es über einen akzeptablen Reifegrad?					
	1.1	Sind Formalien und Verantwortlichkeiten geregelt?	Hoch	Unbewertet	0	
	1.2	Sind adäquate Prozesse und Strukturen geschaffen?	Hoch	Unbewertet	0	
	1.3	Wird ein Sicherheitskonzept gelebt, dokumentiert und ständig verbessert?	Normal	Unbewertet	0	
	1.4	Ist der Sicherheitsprozess in der Organisation verankert?	Normal	Unbewertet	0	
	1.5	Wird die Informationssicherheit ständig überprüft und verbessert?	Normal	Unbewertet	0	
	1.6	Ist ein Managementberichtswesen etabliert?	Niedrig	Unbewertet	0	

Das Sicherheitskonzept



Wo ist SiKoSH ?

- Die Vorgehensweise und alle Hilfsmittel, wie z.B. Richtlinien und Quickchecks stehen zum Download bereit
- Alle SiKoSH-Hilfsmittel sind unter www.sikosh.de verfügbar. Sie sind nach CC BY-NC-SA zur kostenlosen Nutzung freigegeben.

Fisherman's Foe

Warum Phishing so schwer zu bekämpfen ist und wie es doch geht

Beim Phishing kommt etliches zusammen, was Angreifern in die Hände spielt. Unsere Autoren erläutern diese perfide Kombination und was man dagegen tun kann – im Allgemeinen und im Besonderen anhand eines Erfahrungsberichts zum Live-Training in der Landeshauptstadt Kiel.

Von Werner Degenhardt, München, Frank Weidemann, Andreas Amann und Jan Koppelmann, Kiel

Phishing macht Schlagzeilen, mehr oder weniger (un)mittelbar: Am 28. Februar 2018 wurde bekannt, dass im IT-Netzwerk der Bundesregierung Unbefugte ihr Unwesen treiben, möglicherweise schon seit einigen Monaten. Nach allem was man im Moment weiß, führte ein Klick zur falschen Zeit am falschen Ort dazu, dass eine Phishing-Mail ein Stück Schadsoftware in die Hochschule des Bundes in Brühl einschleusen konnte. Dort hat das Programm unentdeckt als „fortgeschrittene, andauernde Bedrohung" (APT, Advanced Persistent Threat) gewartet, bis es Anfang 2017 seine Befehle bekam (vgl. heise.de/-3985590).

Die Bundesverwaltung wirkt insgesamt nervös, die Bundesakademie für öffentliche Verwaltung (BAköV) nahm ihre Lernplattform auf Basis der Open-Source-Software ILIAS „auf Empfehlung des BSI vorsorglich vom Netz" (www.lernplattform-bakoev.bund.de) – die hierüber verwirklichte „Sensibilisierungsinitiative für Informationssicherheit in der Bundesverwaltung" und der BISS-Test zum Erwerb des „Bundes-Informations-Sicherheits-Scheins" (BISS) ruhen derzeit also wegen möglicher Unsicherheit. Kurz vor dem Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) und des neuen Bundesdatenschutzgesetzes (BDSG) am 25. Mai 2018 ist das kein gutes Timing: Denn die DSGVO macht Sensibilisierung und Training von Mitarbeitern nunmehr verpflichtend (Art. 32, 39 und 47).

Mensch, Mensch!

https://www.kes.info/archiv/leseproben/2018/fishermans-foe/

SiKoSH leuchtet ein!

Vielen Dank für
Ihre Aufmerksamkeit

Kontaktadressen:
KomFIT: sikosh@komfit.de