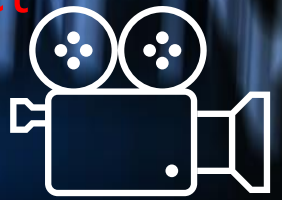
Webcast:
Security im Wandel - neue Gefahren erfordern neue Maßnahmen

Wird aufgezeichnet



Patrick Bärenfänger, Stand: November 2021, V1.1

Patrick Bärenfänger

Lebenslauf

- 1969 geboren, Ausbildung DV-Kaufmann, Studium Elektrotechnik/Informatik
- Seit 1990 in der EDV-Branche
- Von 1995-2001 GAO Münster (Ratiodata IT-Lösungen und Services GmbH)
- 2001 in Projekten für Microsoft, AXA-Colonia, Döres AG, und GAD eG
- Seit Januar 2002 bei der GWS in Münster, Stabstellen in Abteilung TEC und BEW

- Schwerpunkt Informationssicherheit und IT-Ausbildung
  - Verantwortlich für GWS Tech Blog und Syskoportal
  - Modern World: GWS System Requirements, Chefredakteur
  - Cloud Readiness Checks (Analyse und Konzept zur Cloud-Migration)
  - IT-Security Manager und -Auditor (TÜV zertifiziert)
    - IT-Sicherheitscheck nach BSI 200-1 und IDW PS 330
    - Notfallplan und Risiko-Analyse BSI 200-4
  - Systemkoordinierende-Schulung und Zertifizierung
    - RTC Update-Schulungen
    - Administration Azure IaaS und Microsoft 365 Dienste
  - Software Asset Management Workshops
  - Power Apps und Power Automate Entwicklung

Mehr als 30 Jahre IT-Erfahrung

Security im Wandel

neue Gefahren erfordern neue Maßnahmen

Unternehmen müssen sich aufgrund aktueller Bedrohungen auf erweiterte, effektive Werkzeuge und Maßnahmen einstellen. Dieser Vortrag gibt Ihnen einen Überblick über diese neuen Risiken, das Grund-Fundament von Cyber Security. Erfahren Sie über die Möglichkeiten, diesen Gefahren optimal zu begegnen, diese Systemkoordinator-Aufgaben selbst zu lösen oder zu delegieren.

- Bedrohungen
- Cyber Security Essentials
- Maßnahmen
- Firewall 2. Generation mit proaktiven Schutzmechanismen
- Monitoring – Überwachung aller wichtigen Dienste
- Sicherheitsupdates/Software-Aktualisierungen
- Weitere Sysko-Aufgaben (laut Stellenbeschreibung)

Versicherer verweigern den Abschluss von Cyber-Versicherungen bei Nichterfüllung von Standards

Grundlagen

Motivation durch Organisationen

- Das Leben im 21. Jahrhundert ist ohne Informationstechnologie kaum mehr vorstellbar. Information und Informationstechnologie haben sich zu den wichtigsten Gütern entwickelt
- Der Schutz von IT-Landschaften wird deshalb immer wichtiger
- IT-Sicherheit entwickelt sich zu einem entscheidenden Wettbewerbsfaktor

> Jedes Unternehmen muss aktiv möglichen Risiken von Datenverlusten, Systemunterbrechungen oder gar Katastrophensituationen (Desaster) durch Maßnahmen im Bereich physischer, logischer und technischer Sicherheit und die Absicherung gegen Katastrophen, die zum Ausfall von Produktionsrechnern führen entgegenwirken und datenschutzrechtliche Vorkehrungen treffen

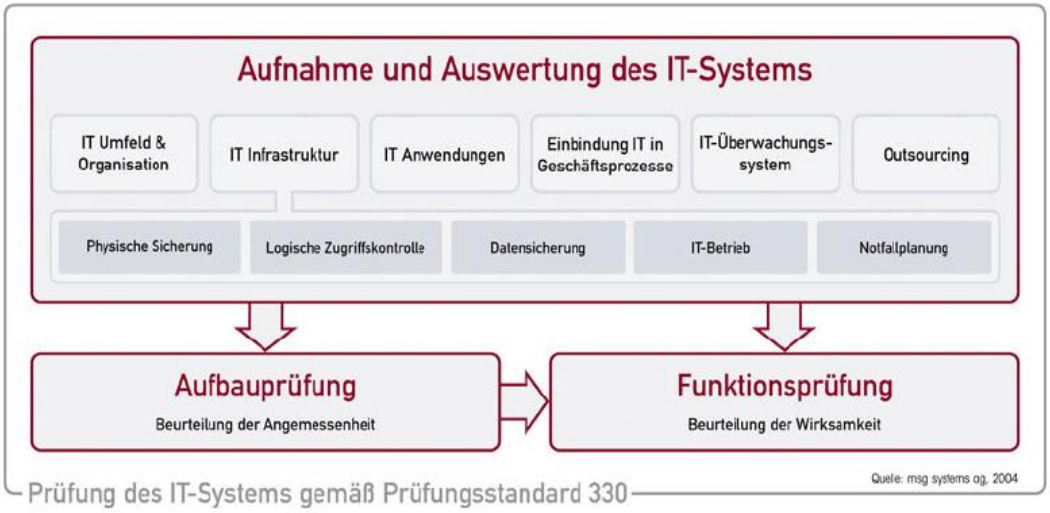
- Diese Rahmenbedingungen und die aktuelle Gesetzeslage tragen dazu bei, die Sensibilität für IT-Sicherheitsthemen zu erhöhen:
  Vorstände und Geschäftsführer sind persönlich für Versäumnisse und mangelnde Risikovorsorge verantwortlich!

Prüfung IT-Systeme – IDW PS 330

Für Compliance-Anforderungen PS 980

Institut der Wirtschaftsprüfer (IDW) Prüfungsstandard 330 (IDW PS 330)

- Im Rahmen von Jahresabschlussprüfungen ist der Abschlussprüfer grundsätzlich dazu verpflichtet, sich mit den (rechnungslegungsbezogenen) IT-Systemen des zu prüfenden Unternehmens zu beschäftigen

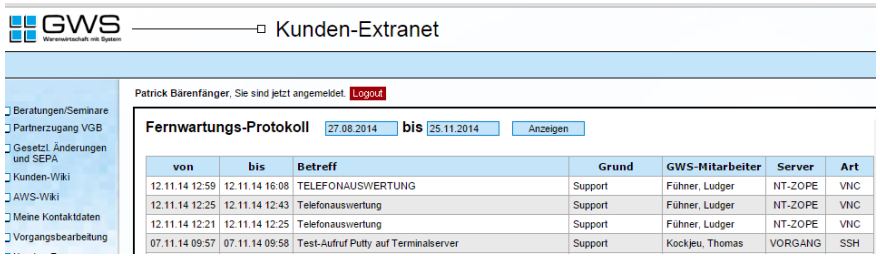


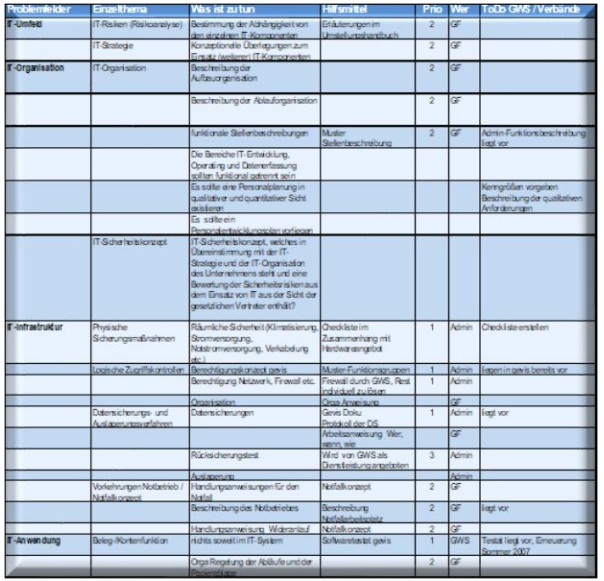
Prüfung des IT-Systems gemäß Prüfungsstandard 330

Gesetzliche Anforderungen

IDW PS330, PS860 und Rating

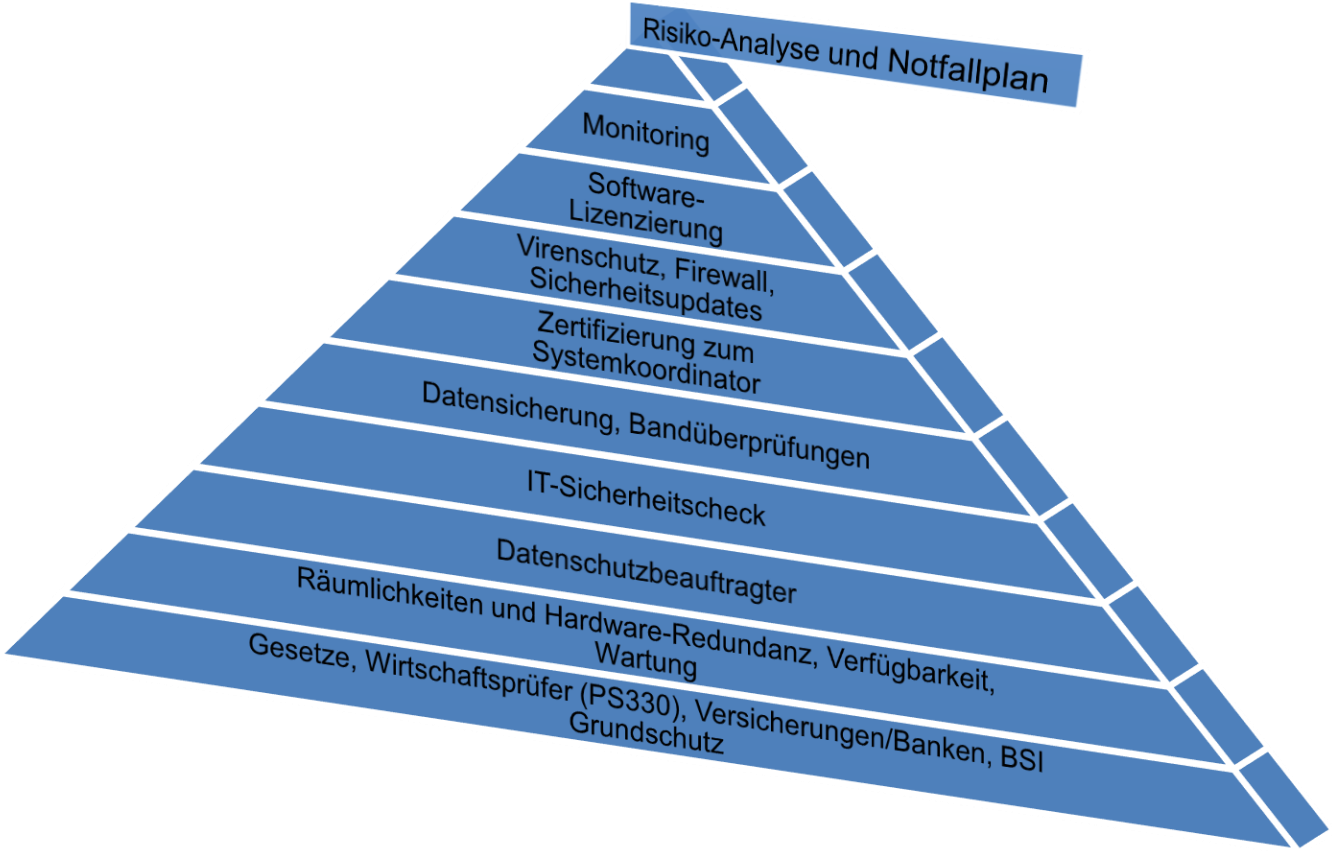
- Handels- und Steuerrecht (§§ 238 ff. und 257 HGB sowie §§ 145 bis 147 AO)
- Ergänzend erlassene Verlautbarungen, wie u.a. IDW PS 330 i.V.m. IDW RS FAIT 1, FAIT 2, FAIT 3, GoBS, GDPdU und ggf. §25a KWG, §4f BDSG
- MaRisk (Mindestanforderungen an das Risikomanagement)
- IT-Sicherheit als Basis für Basel II und Sarbanes-Oxley Act (SOX)
- Auftragsverarbeitung: Vertrag mit Anbietern haben:
  - GWS Rahmenbedingungen Fernwartung, ADV-Vertrag





GWS IT-Sicherheitspyramide

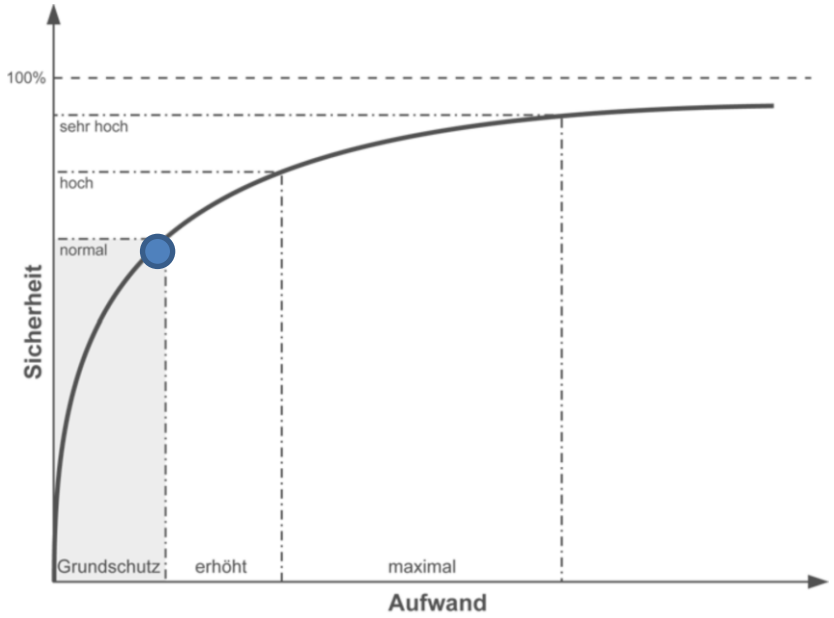
Jede Schicht muss dokumentiert und erfüllt sein



Mindeststandards

Kosten/Nutzen Betrachtung

- Grundschutz muss erreicht sein (Quelle der Grafik: BSI GS Katalog 200-2)
- Die Position des blauen Punkts
  ist Pflicht, mehr zu machen
  ist nicht unbedingt viel teurer
- Unternehmens-Sicherheitsrichtlinie



Allgemeine Sicherheitsthemen

Übersicht/Agenda

- Aktuelle Sicherheitslage und Gefahrenklassen
  - Presse und Sicherheitsradar
- Nachwirkungen Ablauf von abgekündigten Windows, Windows Server, Office und Exchange Versionen
  - Virenschutz, End-of-life alter Versionen
  - wie kommt man als Hacker "rein", Gewichtung nach Verfahren/Risiko
- Mobile Geräte Android, IOS (und deren alte Versionen)
  - Welche Gefahren und Risiken gibt es?
  - wie hält man die Plattformen möglichst sicher (+Kosten/Nutzen)
- Mobile Windows Geräte (Notebooks, tablets)
  - Daten auf mobilen Geräten, unterschiedliche Sicherheitsklassen
- Gefahren im Internet-Betrieb (Zugangsarten, E-Mail, Surfen, Plug-Ins
  - Passwortsicherheit
  - WLAN-Sicherheit
  - Online-Shop als Admin sicher halten, Kunden zu Sicherheit motivieren
  - Homepage auf Sicherheit prüfen – Tipps
  - Zugriffsprotokollierung, wo lässt sie sich mit Bordmitteln nutzen bzw. einschalten
  - Regelmäßige Pflichtaufgaben und Termine
  - Informationsquellen (wie hält man sich auf dem Laufenden)
  - indiv. Sicherheitsstrategie bei IT-Sicherheitscheck erarbeiten)

Aktuelle Sicherheitslage

Presse

Über 12.000 PCs gesperrt

Trojaner TeslaCrypt legt deutsche Behörden lahm

Erpressungs-Trojaner

HDDCryptor soll Computer von Opfern abriegeln

Erpressungstrojaner Jaff: Vorsicht vor Mails mit PDF-A

IDC: Mehr Angriffe auf IT im Corona-Jahr

Die Marktforscher haben über 200 deutsche Unternehmen

Windows Subsystem für Linux

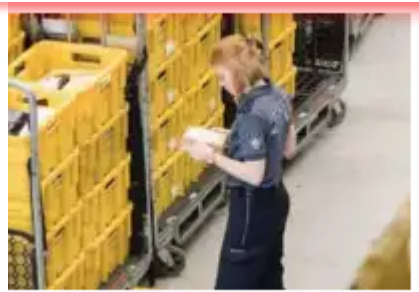
Erste Linux-Malware in Windo aufgetaucht

Was vor vier Jahren noch eine Theorie war, ist nun real: Linux-ELF-Binaries, die Windows-Systeme über deren eigene API angreifen.

Krypto-Virus: Angriff legt 3.100 Server bei MediaMarkt und Saturn lahm

8.11.2021 20:51 Uhr | Frank Hüber

101 Kommentare



"Benachrichtigungen Zoll-Kundendienst": Betrugsmasche greift um sich

Ein Paket hängt beim Zoll fest und kann nur mit Geld losgeeist werden. Das behaupten Betrüger in massenhaft kursierenden E-Mails.

09. Oktober 2020, 09:50 Uhr 235 heise online

Sicherheitslage

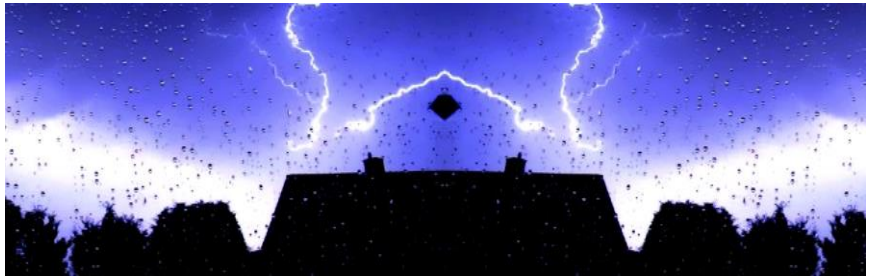
Zahlen und Daten

- 110.000 Bot Infektionen täglich
- Meistens Infektionen auf mobilen Endgeräten
- 114 Millionen neue Schadprogramm Varianten jährlich
- Ransomware: Verschlüsselung der Daten und Lösegeldforderung
- Malware: Umleiten auf andere Webseiten, wirtschaftlichen Schaden zufügen etc.
- Schadcode: Übernahme eines Rechners oder aufbauen von Bot-Netzwerken, um Ziele eingreifen zu können
- Identität stehlen oder übernehmen: Anweisen von Überweisungen, Betrugsversuch

- Super-Spreader: Webshop eines Lieferanten wird übernommen und Schadcode hinterlegt und befällt Besucher und Kunden

- Hafnium: Tausende Exchange-E-Mailserver sind immer noch angreifbar, da zu alt oder/und ohne Sicherheitsupdates

- Angriffe: Automatisierte Benutzer-Anmeldungen aus Indonesien, Russland, USA versuchen Kennwörter zu ermitteln



Akute Bedrohung durch Ransomware und Krypto-Würmer

Verschlüsselungstrojaner/Erpressungssoftware

- Eine E-Mail (die auch von bekannten Absendern stammen kann oder eine Initiativbewerbung ist) enthält einen klickbaren Link auf weitere Informationen. Oder eine Word-Datei
- Klickt der Empfänger auf diesen Link, wird aus dem Internet ein Programm heruntergeladen und auf seinem Rechner ausgeführt. Gleiches wenn er die Word Datei öffnet und Inhalte aktiviert.
- Das Programm verschlüsselt alle Dokumente auf allen Laufwerken (auch Netzlaufwerken), die der Benutzer im Zugriff hat.
- Aktuelle Würmer verbreiten sich und infizieren dann das gesamte Firmennetzwerk
- Lösegeldforderung wird angezeigt (meist zwischen 2000,00 € und 10.000,00 €)

  - Rechner sofort vom Netz nehmen und löschen
  - Nicht auf die Forderungen eingehen! (Empfehlung des Bundesamts für Sicherheit in der IT: BSI)
  - Rücksicherung (wenn 14 Tage aufbewahrt) stellt Daten, die vor Befall da waren, wieder her

Aktuelle Gefahren durch Internetnutzung

Schutz- und Präventivmaßnahmen

- Softwarestand und Sicherheits-Patches auf aktuellem Stand halten (Managed | Server)
- Next Generation Firewall einsetzen (Managed | Firewall)
- Virenschutzlösung aktuell und sicher halten (Managed | Antivirus)
- Zusatz-Datensicherung MEHRERER Generationen in die Cloud (nur wenn ADV-konform)
- Mitarbeiter sensibilisieren, Organisations- und Verhaltens-Anweisung
- Blockieren von Downloads unerwünschter Dateiendungen auf Ihrer w.safe Firewall einrichten
- Alternativen PDF-Betracher, der keine Objekte ausführt, einsetzen (SumatraPDF)
- Kunden informieren (es werden nur noch PDF-Anhänge akzeptiert)
- Exchange Richtlinie einrichten, die unerwünschte Dateiendungen blockiert
- Anzeige von E-Mails in Outlook als "NUR-TEXT"

Gefahrenanalyse und Maßnahmen

Was können wir tun?

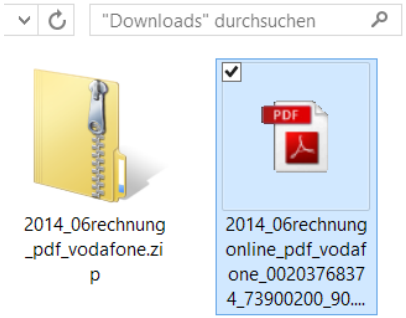
- Risiko-Analyse: Aktuelle Bedrohung durch Erpressungs-Trojaner wie Emotet und Varianten
- Hinter den Kulissen: Wie funktioniert Ransomware der neuen Generation?
- Erste Hilfe: Was ist noch zu retten?
- Backups: Ist mein Backup-Konzept wirklich Trojaner-sicher?
- Richtig vorbeugen: Was hilft wirklich und was bietet nur begrenzten Schutz?
- Altlasten: Was tun mit Windows 7, Server 2008 R2, Exchange, Office 2010

Angriffe in der Praxis

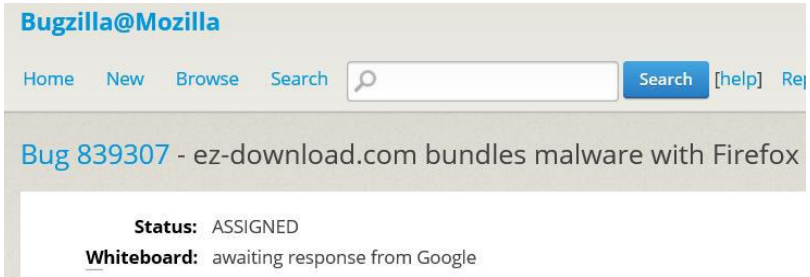
Szenarien

Tägliche Angriffe

Internet/E-Mail

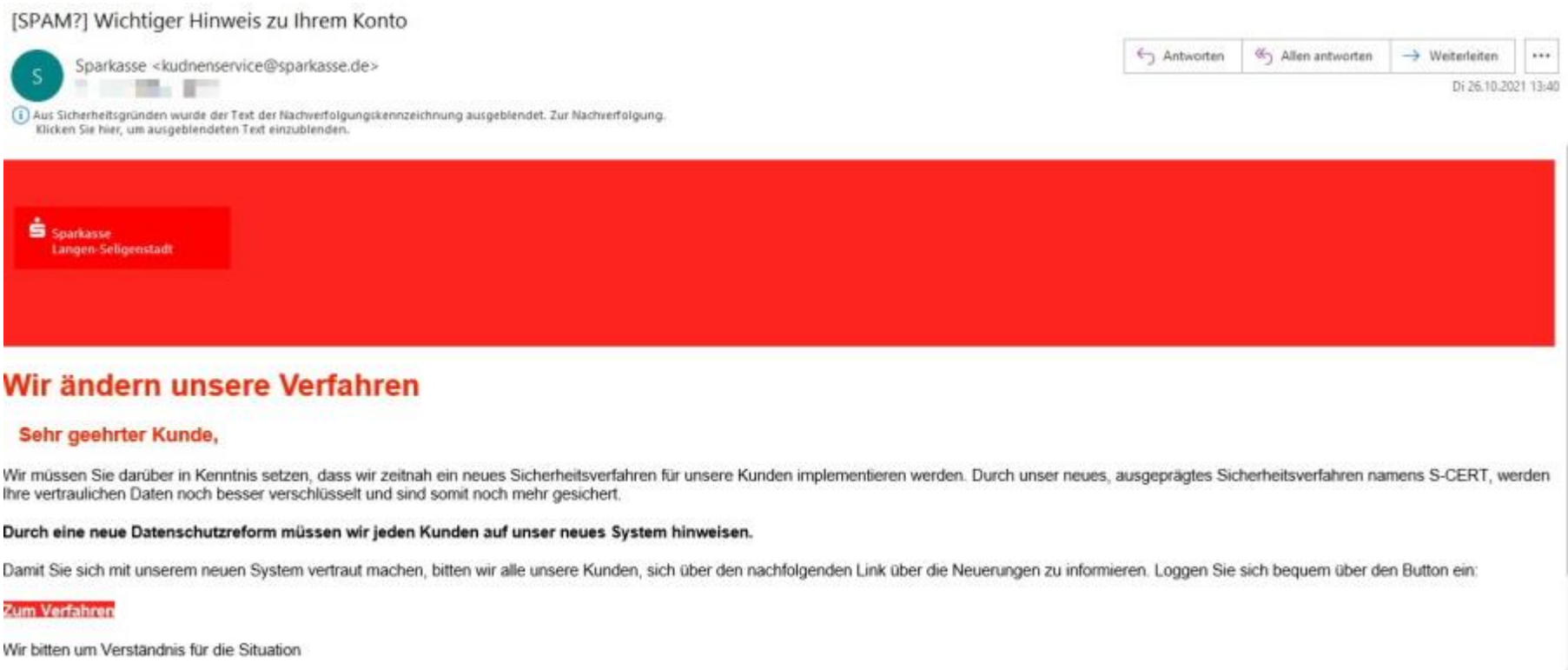


EXE-Datei als PDF mit falschem Symbolbild getarnt



Weiteres Beispiel

E-Mail der Spasskasse – vom „Kudnenservice“ mit Link



[SPAM?] Wichtiger Hinweis zu Ihrem Konto

S Sparkasse <kudnenservice@sparkasse.de>

Antworten | Allen antworten | Weiterleiten | ...

Di 26.10.2021 13:40

Aus Sicherheitsgründen wurde der Text der Nachverfolgungskennzeichnung ausgeblendet. Zur Nachverfolgung. Klicken Sie hier, um ausgeblendeten Text einzublenden.

Sparkasse Langen-Seligenstadt

Wir ändern unsere Verfahren

Sehr geehrter Kunde,

Wir müssen Sie darüber in Kenntnis setzen, dass wir zeitnah ein neues Sicherheitsverfahren für unsere Kunden implementieren werden. Durch unser neues, ausgeprägtes Sicherheitsverfahren namens S-CERT, werden Ihre vertraulichen Daten noch besser verschlüsselt und sind somit noch mehr gesichert.

Durch eine neue Datenschutzreform müssen wir jeden Kunden auf unser neues System hinweisen.

Damit Sie sich mit unserem neuen System vertraut machen, bitten wir alle unsere Kunden, sich über den nachfolgenden Link über die Neuerungen zu informieren. Loggen Sie sich bequem über den Button ein:

Zum Verfahren

Wir bitten um Verständnis für die Situation

Angriffsmethoden und Ziele

Beliebte Hackmethoden

- PC ist auch offline (nicht am Internet angeschlossen) gefährdet!
  - Funkmodul, in Hardware heimlich integriert oder als USB-Stick getarnt
- Spähsoftware
  - Per Mail (z. B. getarnt als Blindbewerbung an die PA), Webseite, USB-Stick
  - Funkverbindungen abhören (auch „Internet-Gastzugang“ für den Besucher)
  - Getränkeautomat mit Internetanschluss
- Smartphones
  - mit eingebautem Spion
  - kostenlose APPS
- Gefälschte Telefonanrufe eines „Kollegen“
- Mitarbeiter als Datenlieferant
  - Abwerbung durch Konkurrenz, Spione als Werksstudent getarnt
  - Soziale Netzwerke

Zitat aus heise-News: „Auf einer billigen Kopie des Samsung Galaxy ist ab Werk installierte Spionagesoftware entdeckt worden. Diese lässt sich so gut wie nicht entfernen, kann alle persönlichen Daten des Nutzers kopieren und Anrufe belauschen.“

Gefahrenklassen

Bereiche mit Sicherheitslücken

- Im täglichen Geschäft nutzt man folgende Geräte
  - Windows PC, Notebook, Windows Tablet
  - Firewall
  - Netzwerk, Windows Datei/Druck-Server/Warenwirtschaft/Terminalserver/Exchange Mail/Fax
  - Android-Smartphones, apple iphone, Windows phone 8 Smartphone (Lumia/Samsung/HTC)
  - Android und apple Tablets

- Netzwerk-Arten
  - Verkabeltes Netzwerk
  - Wireless LAN
  - Mobilfunkdaten (Edge, LTE und 5G)
  - Öffentliche Netze wie Internet, Semiprivate Netze Extranet, Firmeneinwahl über VPN-Tunnel

- Software (Client)
  - Apps (ios, android, Browser-Apps)
  - Browser, Mailprogramm, Oracle Java, Adobe Reader*), Virenscanner, Anwendungen, Betriebssysteme

*) es gibt Alternativen, um auf diese drei Programme zu verzichten

Gefahrenklassen 2

Benutzerverhalten

- Verhaltensregeln für Benutzer (Organisations-Anweisung muss her!)
  - Beim Surfen
  - Beim Benutzen von Portalen, Shops und Seiten mit Anmeldung
  - Sichere und unsichere Seiten
  - Passwörter von Geräten und Webseiten und Portalen bei Onlinediensten
  - Umgang mit Geräten und Daten (insbesondere vertraulichen Daten)
  - Beachten von Gesetzen wie BDSG

Gefahrenklassen 3

Administrator hat noch mehr zu beachten

- Betriebssystem- und Anwendungs-Software mit Sicherheitslücken bzw. wenn EOL ersetzen
- Firewall-Pflege, Regeln, concept of proof, Aktualisierung
- Virenschutzkontrolle und Maßnahmen, Aktualisierung
- Freigabe von Software, Pflege der Software- und Apps Liste und Versionierung
- Datensicherungsprüfung und Verwaltung, Backup und Restore, Brandschutzübungen
- Mailsicherheit, Regeln, Compliance-Einstellungen auf dem Exchange Server
- Smartphones Typen festlegen, absichern, aktuell halten und Stichprobenkontrollen durchführen
- Windows- und Drittsoftware-Patches gegen Sicherheitslücken
- Betrieb von eigenen Shops und Webseiten: Sicherheitslücken stopfen, Software aktuell halten
- Sichere Webseiten betreiben: SSL-Typ und Zertifikate pflegen

Next Generation Managed | Firewall

Erweiterte Technologien zur Prävention und zum Schutz

Funktionsüberblick

Managed | Firewall (am Beispiel Barracuda)

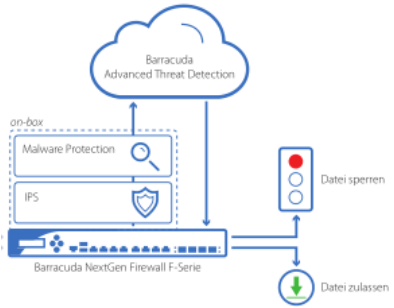
- schützt vor direkten Zugriffen von außen
- Internet-Seiten lassen sich auf Basis des Namens blockieren
- HTTP-Downloads lassen sich nach Endung blockieren
- Proxy-Server lässt nur wenige Türen nach außen offen und leitet weiter
- Optionale Basis-Protokollierung der Surfzugriffe möglich
- Stellt Fernwartungsschnittstelle nach aktuellen Sicherheitsstandards und mit Compliance zur Verfügung
- Bietet verschlüsselten Transportweg für EDI und Verbundkommunikation
- **Prüfen von HTTP und HTTPS Verkehr auf Viren und Trojaner (SSL-interception)**
- **Scannen von Malware auf der Firewall, bevor es den Benutzer erreicht.**
- **Scannen von Virenscanner auf der Firewall, bevor es den Benutzer erreicht.**
- **Sandbox-Verfahren - Hochladen von potenziell gefährlichen Downloads**
- Zulassen oder sperren von z.B. Youtube Videos oder Facebook Nachrichten (Applikationsebene)
- Kanalbündelung von mehreren verschiedenen Internetleitungen (Bandbreite/Ausfallsicherheit steigern)
- Clusterfähig (Hochverfügbarkeit der Firewall)
- VPN-Standortvernetzung (Managed | vpn access)

Managed | Firewall - Firewall der 2. Generation

Merkmale

- Zentrales Management aller Firewalls durch die NetGo, dezentrale Geräte vor Ort, Sicherung der Konfiguration
- Integration in Monitoring (Managed | Monitoring)
- Software für die Verwaltung/Einsicht in Logs durch den Sysko

- Als Basis wird die leistungsfähige Hardware von Barracuda Networks verwendet
- Spezifische Anforderungen wurden angepasst



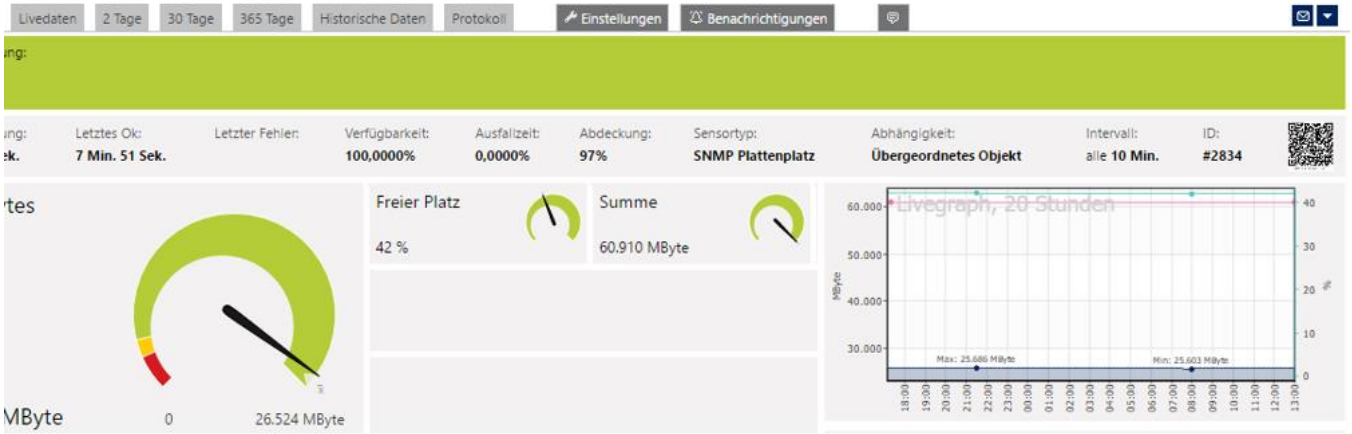
Managed | Monitoring CarePackages

Nächste Generation der Prozess und Betriebsüberwachung

Managed | Monitoring – Monitoring der 2. Generation

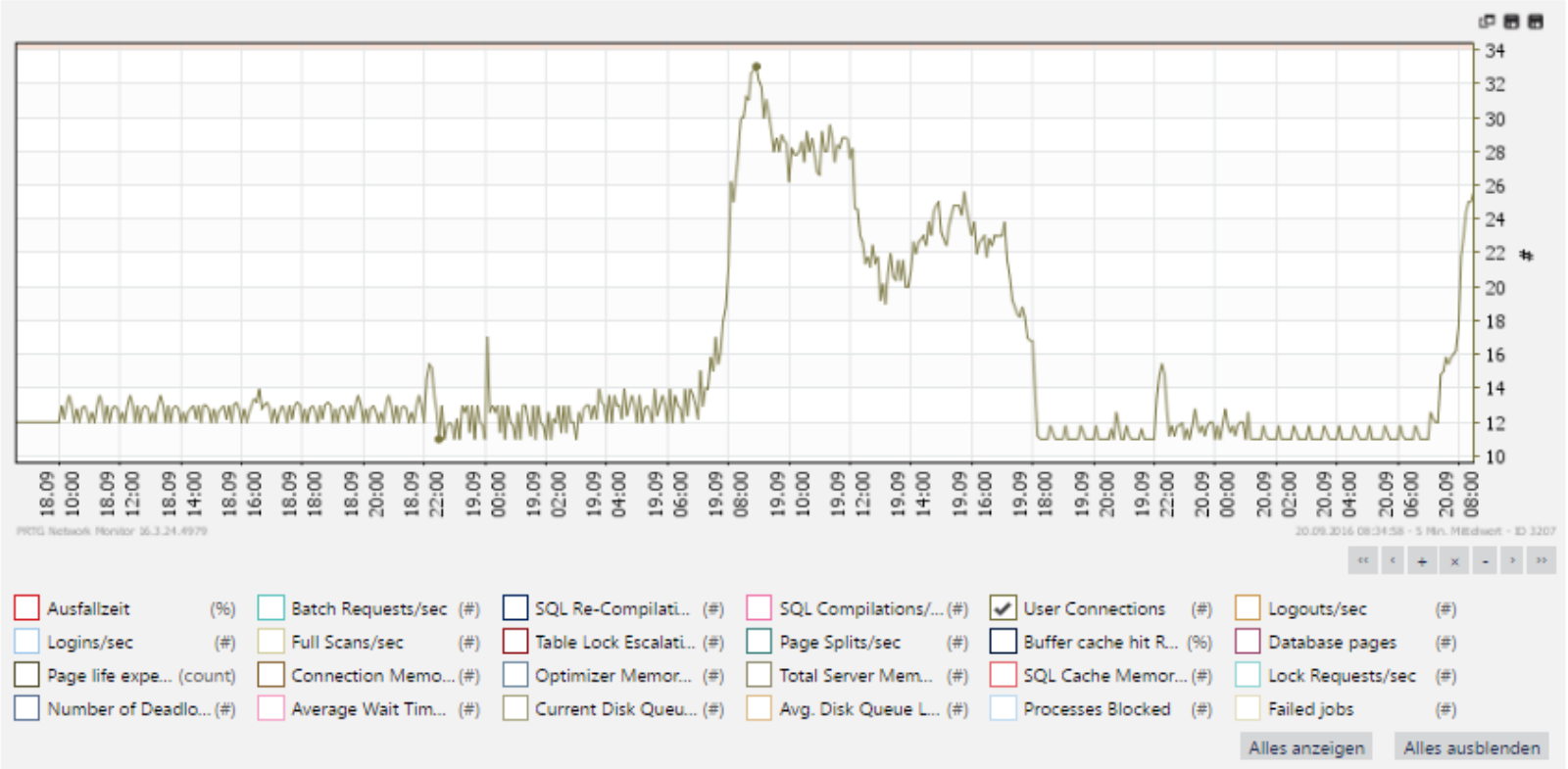
Ziele und Anforderungen

- Vereinfachung der Gesamtsituation
- Manuelle Arbeiten automatisieren, Störungen im Vorfeld erkennen
- Überblick über alle Systeme, Prozesse und Dienste
- Mobilen Zugriff ermöglichen (Android und iOS)
- Historische Daten erkennen, Verfügbarkeit grafisch darstellen
- Produkt basiert auf PRTG Monitoring (Lizenzprodukt)
- + GWS-Erweiterungen und Implementierung für gevis ERP und Dienste
- + Monitoring durch die GWS und definierte Aktionen



Managed | Monitoring

Historische Daten



Zusatz-Datensicherung in der Cloud

Hochverfügbar, compliant, Langzeitsicherung, sicher

Datensicherung auslagern

Für On-Premises und Hybrid IaaS Szenarien

- Mit Managed | Cloud VM-Backup haben Sie die Möglichkeit, Ihre OnPrem Umgebung oder auch die gevis ERP Datenbank in der Cloud zu sichern. Hierdurch erfolgt eine geographische Auslagerung Ihrer Backup-Infrastruktur außerhalb Ihres Standortes. Die Sicherung übernimmt die Datensicherungssoftware Veeam und wird mithilfe von Monitoring überwacht. In einem Fehlerfall behebt die GWS den Fehler und sorgt dafür, dass das Backup schnellstmöglich stabil und ordnungsgemäß funktioniert.

- Die Aufbewahrungsrichtlinie wird in Abstimmung mit Ihnen definiert und ist flexibel gestaltbar (Tages-, Wochen-, Monats-, Jahressicherung). In einer kleinen Analyse wird vorab geprüft, ob Sie für die zu sichernden Daten über einen ausreichenden Internetanschluss verfügen.

- Voraussetzungen:
  - Aktuelle veeam Backup & Recovery Version auf On-Prem-Servern, Lizenzen und Speicherplatz in Microsoft Azure (Region West Germany)
  - Breitband-Internet-Verbindung ab 50 Mbit Upstream (je nach komprimierter Datenmenge)

Server sicher in der Azure Cloud mieten

Statt Neuanschaffung und teurer zusätzlicher Sicherheitsmaßnahmen

Microsoft Strategie: Cloud first

Was ändert sich?

- Release-Zyklen der Produkte und Abhängigkeiten verkürzen sich von 10 Jahren auf 7, teilweise auf 3 Jahre

- Einmal pro Jahr erscheint eine neue Version von Dynamics 365 Business Central

- Beispiel: Microsoft Dynamics 365 Business Central Version 180 könnte nicht mehr vollständig kompatibel sein mit Microsoft Office 2016

- Software-Lizenzen von Windows Server, Windows, Office und anderen Produkten nur noch mit Software-Assurance Wartungsvertrag, ansonsten alle 3 Jahre neu kaufen
- Office Kaufversionen erhalten nur noch 5 Jahre Sicherheitsupdates (statt 10)

- BSI Grundschutz-Anforderungen an Serverräume und Datenverfügbarkeit und Einhaltung Datenschutz sind erhöht und werden von Versicherungen und Behörden verstärkt verfolgt:
  - Vielfach ist kein Serverraum vorhanden, der die Ansprüche erfüllt und kein separater Raum für die Datensicherungsgeräte

Microsoft Strategie: Cloud first

Wie geht man das am besten an?

Wege zur Entscheidung: Cloud oder On-Premise (Server im Hause):

- Cloud Readiness Check
  - https://tech-nachrichten.de/schulung-cloud-readiness-check/
  - sammelt Daten und bereitet sie zur Beurteilung der Entscheidung auf.

- Entscheidung wird getroffen:
  - Hardware-Investition und Baumaßnahmen zum Erreichen von BSI-Grundschutz
  - Server-Modernisierung

  oder (wenn nicht vermeidbar: Hybrid-Betrieb)
  - Anmietung von Cloud-Infrastruktur und Softwarelizenzen (Microsoft Azure)
  - Aufbau der Infrastruktur in der Cloud (IaaS)

  oder
  - Gevis ERP aus der Steckdose (SaaS), die Browser-Anwendung wird quasi wie eine Banken-Seite zur Verfügung gestellt.

Mobile Geräte verwalten

Compliance erreichen, Smartphones inventarisieren und verwalten

Mobile device Management

- Was sind „Mobile devices“?
  - Notebooks und Tablets mit Windows Professional Betriebssystemen
  - Apple tablets (z.B. ipad, ipad mini und ipad air)
  - android tablets (z.B. Samsung Galaxy tab)
  - Android Smartphones ab android 4 (Marktanteil über 84% weltweit, z.B. Samsung Galaxy Serie)
  - Apple Smartphones ab iphone 4 (Marktanteil ca. 15% weltweit, ältere Geräte nicht gut managebar)

- Beim Management der mobilen Geräte geht es grundsätzlich darum:
  - Geräte zu erfassen
  - die Software und Daten darauf auf dem aktuellen Stand zu halten und
  - die Unternehmensdaten auf den Geräten zu schützen.
  - Quelle: Marktanalyseunternehmen Strategy Analytics, Stand: Mai 2016

Mobile Device Management

Wo liegt der Nutzen? Warum benötige ich das?

- Bundesamt für Sicherheit und Informationstechnik (BSI) hat Leitfaden für Mobile Geräte erstellt und in den Grundschutz integriert → Grundschutz muss jedes Unternehmen erfüllen

- Szenarien:
  - Gerät wird gestohlen → Daten können gelöscht und das Gerät gesperrt werden
  - Mitarbeiter haben die PIN abgeschaltet → Richtlinien verhindern das
  - Geräte sollen im Inventar erscheinen (welcher Mitarbeiter hat welche Geräte im Einsatz)
  - Firmenspezifische Apps stehen bei den Stores im Vordergrund

Was kann verwaltet werden?

Mobile Device Management Möglichkeiten

- Generelle Absicherung
  - Versicherungen (z.B. vodafone RED, R&V, lenovo) Diebstahl, Glasbruch, Verlust (haften optional auch bei leichter Fahrlässigkeit)
  - Virenschutzprogramme (Kaspersky - Windows: Pflicht, android: optional)
  - Organisationsanweisung trotzdem erforderlich, nicht alles kann technisch gelöst werden

- Windows 10-Pro-Geräte (z.B. lenovo Thinkpad Yoga X Serie oder Microsoft Surface Books Pro):
  - Inventarisierung und regelmäßiges Scanning von installierter Software und Hardware möglich mit Open Source Software auf dem Server
  - Unternehmensrichtlinien (Domänen-GPOs) möglich mit Bordmitteln
  - Zentrale Vergabe von Berechtigungen (Domain policy und NTFS rights)
  - Einschränkung der Windows 8.x modern Apps per Richtlinie
  - Verschlüsselung (Bitlocker) von Partitionen, zentral nur mit Software Assurance!

- **Empfehlung:** Microsoft InTune (auch in Verbindung mit SCCM) Windows android IOS:
  - https://www.microsoft.com/de-de/server-cloud/products/windows-intune/default.aspx#fbid=XOLvlk4JDKJ

Webseiten und Shop betreiben

Szenarien, Gefahren und Maßnahmen

DSGVO und Cookie-Gesetze

Abmahn-Gefahr!

- Seit Mai 2018 ist die Datschutzgrundverordnung aktiv und erweitert die Vorgaben aus dem Bundesdatenschutzgesetz
- Seit 28. Mai 2020 ist die EU-Cookierichtlinie mit dem höchstrichterlichen BGH-Urteil in deutsches Recht umgesetzt worden.
  - Cookies dürfen nur noch gesetzt werden (außer technisch notwendige), wenn der Besucher dem zustimmt
  - Besucher müssen über Umfang Art und Klasse, sowie den Zweck der Cookies informiert werden (Cookie-Banner mit Ablehnungsoptionen)

- Bei Verstößen ist mit Abmahnungen und Bußgeldern zu rechnen

Szenarien und Gefahren

Shop- und Webseiten-Betrieb

- Webseiten und Shops können in Eigenregie technisch betrieben werden → großer Aufwand (Firewalls, DMZ, Internetleitung, Bandbreit, Volumen, Shopsoftware, Plattform, Serverhardware und Redundanz)
- Daher werden Webseiten und Shoplösungen meist bei einem Anbieter gemietet, dieser kümmert sich um Verfügbarkeit, Hardware und Bandbreite und Sicherheitsupdates

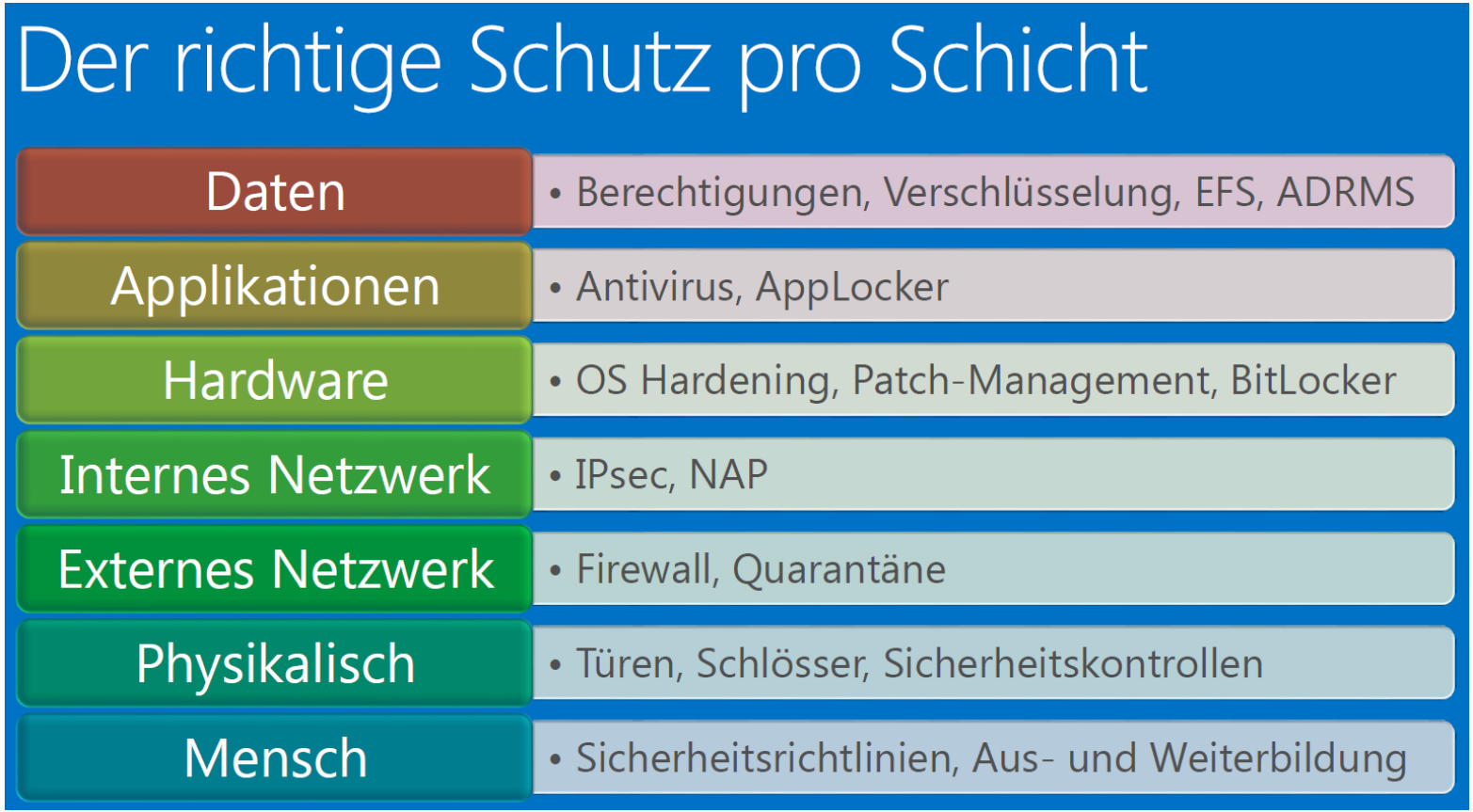
- Die Verwaltung bleibt bei Ihnen:
  - Sie legen Ihre Kunden als Benutzer im Shop an ← sichere Passwörter https://asp.gws.ms/passwortgen.asp
  - Sie verwalten die Inhalte, Artikel, Bilder und Preise (Urheberrecht bei Bildern beachten)
  - Sie stellen ggf. Dokumente (Rechnungen, Belege) Ihren Kunden zur Verfügung (Datenschutz bearbeiten und Dokumente sicher bereitstellen)
  - Sie pflegen die Inhalte Ihrer Website mit einem Content Management System (CMS) ← rechtliche Grundlagen beachten
  - Sie haben Adminzugriffe auf Verwaltungsoberfläche von Web, CMS und Shop ← Sichern Sie Ihr Passwort besonders und ändern es alle 30 Tage

Fazit, GWS-Unterstützung

...und Literaturhinweise

Zusammenfassung Schutz mit Bordmitteln

Aufgaben



Fazit

„Best practice“

- Beginnen mit Bordmitteln, prüfen ob Anforderungen gedeckt
- Organisationsweisungen und Verhaltenshinweise müssen die technischen Methoden ergänzen
- Der Benutzer ist und bleibt die größte Gefahrenquelle
- Stichproben durchführen (muss auch vertraglich abgesichert sein)
- Netzwerk und lokale Plattform stetig aktualisieren, Lücken schließen
- Eigene Firewall ständig aktualisieren und anpassen
- Webplattformen mit sensiblen Daten auf SSL umstellen, Lücken schließen oder Serviceverträge mit Anbietern (SLA) schließen
- Kaufsoftware für mobiles Geräte-Management erwägen

IT-Sicherheits-Check

Gutachten

- „Erfüllt Ihre EDV-Landschaft die Grundvoraussetzungen?“ - Nach einem Tag wissen Sie es!
- Umfassender Check (Basis: Grundschutzkataloge BSI und IDW Prüfungsstandard 330) durch **TÜV-geprüften IT-Security-Manager und Auditor**
- Sicherheits-Check wird gemeinsam mit dem SYSKO durchgeführt

- Nutzen:
  - Protokoll und Bericht (einschließlich Maßnahmenkatalog) als Ergebnis
  - Tipps & Tricks
  - Reduzieren Sie den Umfang des Mängelreports des Wirtschaftsprüfers
  - Herstellung eines sicheren Zustandes und Erläuterung von Werkzeugen, die dabei unterstützen

https://tech-nachrichten.de/schulung-it-sicherheits-check-workshop/

Notfallplan und Risiko-Analyse

BSI Standard 200-4, aufbauend auf dem IT-Sicherheitscheck 200-1

- Der Notfallplan mit Risiko-Analyse ist ein auf Basis von BSI-Standards 200-3 und 4 erstelltes Regelwerk, das bei Ausfällen Anleitungen der IT-Umgebung Maßnahmen beschreibt und bewertet. Auf Basis der vorhandenen Infrastruktur und Geschäftsprozesse werden Daten gesammelt, die Prozesse gemeinsam beleuchtet und eine Risikoeinschätzung vorgenommen.
  Ziel ist die Ermittlung eines Schätzwertes: Kosten in EURO pro Stunde Betriebs-Stillstand nach Schadensklassen und nach Geschäftsprozessen gegliedert.
  Zu den Schadensklassen und Geschäftsprozessen wird dokumentiert, wie bisher Vorsorge getroffen wird, um den Schaden abzumildern bzw. komplett abzufangen und was im Schadensfall zu tun ist

https://tech-nachrichten.de/schulung-notfallkonzept-risiko/

Hybrid-Szenario

Zusatz-Datensicherung in der Cloud

- Ihre auf dem On-Premises (in Ihrem Hause) betriebene Datensicherung um eine Zusatzsicherung in der Cloud erweitern
- Wichtige Daten sind unter höchster Sicherheit und verschlüsselt im K-Fall abrufbar
- Ergänzung zur Bandsicherung/NAS-Kopie in anderem Brandabschnitt

https://gws.ms/sicher-ist-sicher-managed-cloud-vm-backup/

Managed | CarePackages

IT-Betrieb und Sysko-Tätigkeiten auslagern

- Es herrscht Fachkräftemangel im IT-Bereich
- Systemkoordinierende erfüllen Ihre Aufgaben als Nebentätigkeit
- Bei geschäftskritischen Ausfällen wird reagiert, statt proaktiv zu agieren
- Sysko-Aufgaben und Monitoring bleiben auch bei IaaS Cloud-Betrieb bestehen

https://gws.ms/managed-services/

Server sicher in die Cloud statt Server neu kaufen

Cloud Readiness Check | Azure

- Im Zuge der Digitalisierung ist eine verfügbare und jederzeit betriebsbereite IT-Umgebung essenziell. Gesetzliche Vorgaben fordern, immer auf aktuellem Stand zu sein. Die Hardware muss mit Ihren Betriebsanforderungen und Aufgaben wachsen. Nahezu alle führenden Software-Hersteller verkürzen ihre Support-Zyklen, um dem technischen Wandel Schritt zu halten. Bisher haben Sie alle 5 Jahre eine 5-6-stellige Investition in neue Hardware und Software getätigt. Hardware und Dienste in die Cloud zu verlagern ist im Vergleich dazu eine Möglichkeit. Erfahren Sie, wie weit Ihre Umgebung oder Teile davon zukunftssicher und wirtschaftlich der Digitalisierung und dem Softwarewandel mithalten kann.

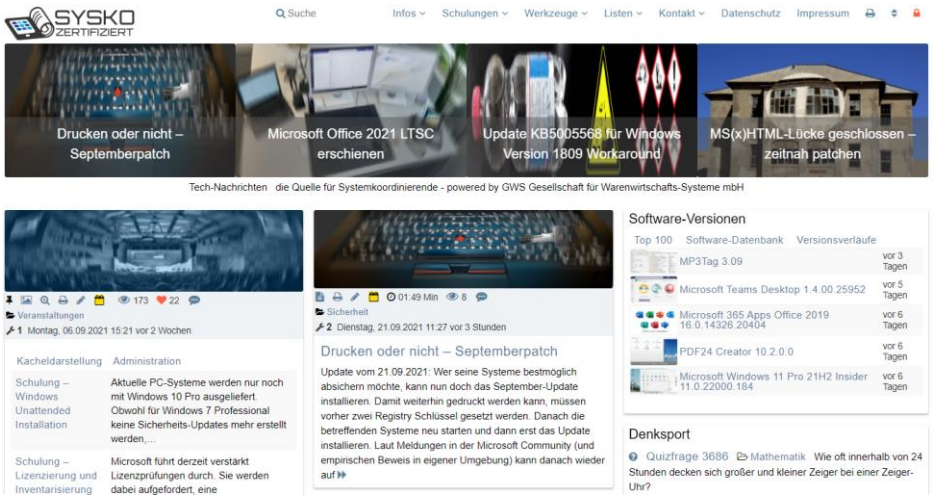
- Das Fundament für ein zukunftsfähiges IT-Konzept bildet der Cloud readyness check (CRC). Dieses Strategiepapier zeigt Ihnen anhand der ermittelten Infrastruktur detailliert auf, inwieweit Sie Cloud-fähig sind in welche Richtung Sie Ihre IT-Strategie und -Umgebung ausrichten können

https://tech-nachrichten.de/schulung-cloud-readiness-check/

Quellennachweise

Nützliche Referenzlinks

- Sysko-Portal ← Nachrichten für den Systemkoordinator und zur IT-Sicherheit
- Alles zum Systemkoordinator (mit Video) im Sysko-Portal: https://tech-nachrichten.de/informationen-fuer-systemkoordinatoren/
- heisec.de ← Heise Sicherheitsticker informiert über aktuelle Lücken
- https://bsi.bund.de ← Bundesamt für Sicherheit
- Video und Präsentation sind im Sysko-Portal herunterladbar: Kennwort: **sind S1e sicher?**



Vielen Dank für Ihre Aufmerksamkeit! Zeit für Ihre Fragen

Ihr Feedback bitte QR-Code scannen:

Patrick Bärenfänger
IT-Security-Manager und Auditor (TÜV)
Branchensoftware-Entwicklung

Tel: +49 (251) 7000-3896
Fax: +49 (251) 7000-3999
patrick.baerenfaenger@gws.ms

https://tech-nachrichten.de/feedback/?Veranstaltung=webcast-security-im-wandel&verandatum=2021-11-12