KISA

IT? Aber sicher!

Erfahrungsbericht des Informationssicherheitsbeauftragten von KISA

Marcus Kurth
Radebeul, den 28. Februar 2018

KISA

„Das einzige sichere System müsste ausgeschaltet, in einem versiegelten und von Stahlbeton ummantelten Raum und von bewaffneten Schutztruppen umstellt sein.“

Gene Spafford

Professor Purdue University

KISA

Agenda

1. kurzer Überblick zur Informationssicherheit
   - Was ist zu schützen?
   - unsere Erfahrungen aus den Verwaltungen

2. Wenn das Worst-Case-Szenario Wirklichkeit wird – was tun im Katastrophenfall?
   (Albert Sturm, Stadt Straubing)

3. Unsere Unterstützungsleistungen für Sie

KISA

Was ist zu schützen?

Informationen …

- sind wertvolle Werte, die geschützt werden müssen.
- müssen unabhängig von ihrer Form sowie der Art ihrer Nutzung und Speicherung - angemessen geschützt werden.

Diese findet man

- im Netzwerk, auf Speichermedien und mobilen Systemen,
- in Papierform und
- in den Köpfen der Mitarbeiter.

KISA

Unsere Erfahrungen

- Ø Ergebnis unserer letzten 10 QuickChecks Informationssicherheit lag bei 42,93 %

- häufig festgestellte Mängel
  - alleiniges Vertrauen auf technische Maßnahmen
  - kaum fixierte organisatorische Regelungen
  - unzureichende Sensibilisierung der Mitarbeiter
  - geringe Bewertung der Bedeutung der IT für den Arbeitsalltag

„Uns wird schon nichts passieren!“

KISA

Agenda

1. kurzer Überblick zur Informationssicherheit
   - Was ist zu schützen?
   - unsere Erfahrungen aus den Verwaltungen

2. Wenn das Worst-Case-Szenario Wirklichkeit wird – was tun im Katastrophenfall?
   (Albert Sturm, Stadt Straubing)

3. Unsere Unterstützungsleistungen für Sie

STADT STRAUBING

Brand im Straubinger Rathaus
am 25. November 2016

Kommunale Informationsverarbeitung Sachsen
Kundenforum am 28. Februar 2018

Schadensverlauf

- Kreisfreie Stadt Straubing
- Einwohner: 50.000
- Standorte: 20
- PC-Arbeitsplätze: 600
- Zentrales Rechenzentrum im Rathaus


RZ 2
Gebäudekomplex
Seminargasse
RZ 1
Gebäudekomplex
Simon-Höller Strasse
Zentraler Hausanschlußraum
mit Hybrid TK-Anlage

Schadensverlauf

» Das historische Rathaus stand bereits kurz nach Feueralarm im Vollbrand.
Der Brand entstand außerhalb der Kernarbeitszeiten Freitag, den 25.11.2016 gegen 15:45 Uhr.


Lebkuchen-Schmidt aus Nürnberg


HALLER
Zimmerei · Holzbau
KERSCHER


adventskalender


Lentner


HALLER

Schadensverlauf

- Ein Betreten der vom Brand betroffenen Bereiche war nicht mehr möglich.
- Strom- und Telefonanbindungen waren innerhalb kurzer Zeit komplett zerstört. Datenverbindungen waren inaktiv.
- USV und das angesprungene Notstromaggregat versuchten die Stromversorgung intern aufrecht zu erhalten.
- Aufgrund verbrennender Leitungen wurde die IT-Hardware mit Spannungsunterbrechungen, Spannungsspitzen und Kurzschlüssen „bombardiert“.
- Feuerwehr schaltete USV und Notstromaggregat aus, um eine zusätzliche Gefährdung beim Löschen auszuschließen.
  Noch bestehende Leitungen wurden durchtrennt.
- Rechenzentrum 1 lag 30 Meter neben dem Brandherd.
- Die Sicherungsbänder konnten mangels Stromversorgung und Zeitdruck nicht mehr entnommen werden.

Schaden

- Backupserver (im Rack) mit den internen Festplatten konnte „ausgebaut“ werden.
- Stromeinspeisung des Rathauses und Telefonanschluss verbrannt.
- Die Telefonanlage wurde komplett zerstört.
- Zentrales Klimasystem und Gebäudeleittechnik nicht mehr existent.
- Netzwerk Verteiler historisches Rathaus durch Brand vernichtet
- Knapp 1.000.000 Liter Löschwasser im Gebäude verursachten nachhaltige Schäden an nicht abgebrannten Gebäudeteilen und Einrichtungen.
- Die Rechenzentren wurden weder durch Feuer noch durch Löschwasser in große Mitleidenschaft gezogen, es gingen anscheinend keine Daten verloren.
- Zustand der EDV-Systeme überwiegend unbekannt.


HALLER
KIRSCHER

Medaillon Grimm

Wiederinbetriebnahme

- Kein Betreten der vom Brand beschädigten Gebäudeteile möglich, so lange die Polizei die Brandursache ermittelt.
  Schon während des Brandes Absprachen mit LKA und Kripo, welche Areale zum Wiederaufbau der Stromversorgung und der Telefonanschlüsse unter Begleitung der Brandermittler betreten werden dürfen.
- Während des Brandes proaktive Kontaktaufnahme durch unsere strategische Partnerfirma.
  - Bereitstellung eines 24x7 erreichbaren Krisenteams für die Wiederinbetriebnahme.
  - Auf Zuruf sofortige Lieferung aller lagermäßig verfügbaren Hardwarekomponenten.
  - Abruf des gesamten Telefonsystems.
  - Planung einer Laborumgebung im Rathaus für die Inbetriebnahme und Konfiguration der TK-Anlage.
  - Abstimmen der Grundkonfiguration des TK-Systems mit den ausführenden Mitarbeitern.
  - Vorkonfiguration der Anlage im Labor der Firma.
- Nach 24 Stunden Wiederherstellung der Stromversorgung in den nicht zerstörten Bereichen.
- Hochfahren des Netzwerkes. Einige Switche konnten nach den erlittenen Spannungsunterbrechungen/-spitzen nicht gestartet werden. Die Startprozeduren wurden fehlerhaft abgebrochen. Erst nach dem Reset aller Module war der Start möglich. Dabei wurde ersichtlich, dass Teile der Konfiguration verloren gegangen waren, im Nachgang war eine Neukonfiguration erforderlich (Routing, VLans).

Wiederinbetriebnahme

- Hochfahren der Storage-Systeme. Herstellersupport (über den strategischen Partner) war notwendig. Die Synchronisation der beiden gespiegelten Storages dauerte ca. 12 Stunden.
- Die ESX Server versuchten beim Starten alle 100 zuletzt laufenden VMs zeitgleich hochzufahren.
- Die Überlastung der beiden Systeme erzeugte so hohe Latenzen, dass Fibre-Channel Verbindungen zur Storage deaktiviert wurden. Dies musste später manuell bereinigt werden. Die Systeme waren zu diesem Zeitpunkt nicht administrierbar (Status Sonntag 0:00 Uhr).
- Wegen der zerstörten Gebäudeleittechnik lief die inzwischen wieder in Betrieb genommene Heizungsanlage im uneingeschränkten Heizmodus.
  Die Temperatur im Gebäude lag bei ca. 40 ° Celsius.
- Die zentrale Klimatisierung der Serverräume war zerstört. Die Ersatzklimatechnik nach Wartung zwar funktionsfähig aber vom Löschwasser geschädigt. Kurzfristig beschaffte mobile Geräte waren nicht leistungsfähig genug und nicht dauerbetriebsfähig. Die Rechenzentren konnten nur aufgrund der Außentemperatur von -17 ° Celsius dauerhaft in Betrieb gehalten werden. Im Sommer wäre ein Wiederanlauf gescheitert.

Wiederinbetriebnahme

- Installation, Konfiguration (Basiskonfiguration) des neuen TK-Systems und Rollout von ca. 600 Endgeräten durch die strategische Partnerfirma (Lieferung Samstag 26.11.2016, Fertigstellung Mittwoch 30.11.2016).
- Einführen einer einheitlichen Kopfnummer für die gesamte Stadtverwaltung Straubing.
  - Wechsel von 3-stelligen Nebenstellen zu 2-stelliger Standortkennung plus 3-stelligen Nebenstellen.
  - Erneuerung des gesamten Rufnummernplans.
- Ausbau des Datennetzes (Dark Fibre) zur Erschließung von Ersatzbüroflächen.

- Montag, 28. November 2016,
  - 8:00 Uhr Personalversammlung, Information über den Brandschaden.
  - Ab 12:00 Uhr Normalbetrieb in der gesamten Stadtverwaltung.

Warum war die Wiederinbetriebnahme so zeitnah möglich?

- Frühzeitiger Kontakt mit der Polizei erlaubte das begrenzte Betreten des eigentlich gesperrten Areals (Ermittlung der Brandursache). Dadurch war der provisorische Aufbau einer Stromversorgung und Telefonanbindung sowie die Inbetriebnahme der Heizung möglich.
- Der überwiegende Teil der Infrastruktur, die Kernnetzwerkkomponenten und die Rechenzentren waren nicht oder nur leicht von Brand und Löschwasser in Mitleidenschaft gezogen.
- Der Datenbestand war integer, ein Restore war nicht notwendig.
- Proaktive Partnerfirma, der Netzwerk und Serversysteme bekannt sind. Diese handelte auch den Herstellersupport beim Start der Basisdienste, da zu diesem Zeitpunkt noch keine Internetverbindungen (Remote-Support, Austausch von Log-Files) verfügbar waren.
- In der kritischen Wiederanlauf-Phase stand der Support des Partners umgehend und rund um die Uhr zur Verfügung.

Warum war die Wiederinbetriebnahme so zeitnah möglich?

- Kurze Entscheidungswege aufgrund klar geregelter Zuständigkeiten bei einem Schadensereignis in den Bereichen Hochbau, Gebäudemanagement und IuK.
- Das Herunterfahren und Neustarten der gesamten IT war im Rahmen der Brandschutz- und Energiesanierung des Rathauses mehrfach notwendig. Der Ablauf war erprobt, allen Beteiligten bekannt und fast eine Abfolge von Routinehandlungen.
- Systemdokumentation, Config-Files, Tools und Einzelplatzsysteme für die Wiederinbetriebnahme waren unabhängig vom Netzwerk verfügbar.
- Eine neu beschaffte Telefonanlage war zufällig geordert und konnte auch abgerufen werden.
- Die winterliche Außentemperatur ermöglichte einen Dauerbetrieb der Rechenzentren trotz eingeschränkter Funktion der Klimatechnik.

Erkenntnisse, Verbesserungswünsche, offene Probleme

- Ohne Internetverbindung ist ein Herstellersupport beim Hochfahren nicht möglich (Remote, Versand Logdateien per Email, etc.).
- Das Löschwasser ist in Verbindung mit Brandrückständen aggressiv wie eine Säure. Dadurch wurden auch Räume, EDV- und Elektroinstallationen und am Boden stehende PCs, etc. zerstört, die nicht direkt vom Brand betroffen waren.
- Wir wussten, was wir zu tun hatten.
  Für den Bereich IuK: Vollständige Außerbetriebnahme und Wiederhochfahren der IT wurden mehrmals durchgeführt. Der Ablauf war für uns kein Novum.
  Das Herunterfahren und Neustarten der gesamten EDV-Systeme sollte ein Routinevorgang sein. Periodisches Training empfehlenswert.
- Aufteilen neuralgischer Anschlüsse für Strom und Telefon auf mehrere Zugänge, die notfalls auch einzeln die Versorgung der gesamten Gebäudestruktur sicherstellen können.
- Sicherstellen redundanter Kommunikationsstrukturen von den Rechenzentren zu den Clients im Rathaus und den Außenstellenstandorten.

Erkenntnisse, Verbesserungswünsche, offene Probleme

- Zur Vermeidung des vollständigen Ausfalls einer zentralen Telefonanlage, Virtualisierung derselben und Bereitstellung der Services über verteilte Rechenzentren. Katastrophenschutz erhält zusätzlich eigenständige Redundanz.
- Anlässlich eines Brandes oder im Katastrophenfall wird Strom großflächig abgeschaltet, mit der Folge, dass auch bei einem Brand in der Nachbarschaft die zentrale IT im Rathaus stromlos ist (kein Zugriff mehr auf Daten zur Evakuierung (EWO-Bestand), keine Versorgung der Außenstandorte).
  Abhilfe durch Replikation der Backups an einem räumlich entfernten Standort.
- Kurze Entscheidungswege aufgrund klar geregelter Zuständigkeiten bei einem Schadensereignis in den Bereichen Hochbau, Gebäudemanagement und IuK.
- Dokumentation, Inventarisierung der gesamten Hardware, Infrastruktur, Konfigurationen kommt sehr hoher Stellenwert zu. Aktuelle Kopie der abgelegten Informationen zwingend auch extern speichern.

Erkenntnisse, Verbesserungswünsche, offene Probleme

- Spiegelung eines Storage möglichst in anderes Gebäude (u.U. schwierig wegen der notwendigen Bandbreite…).
- Backupserver mit NAS möglichst in anderen Brandabschnitt, weit weg von Storage/Servern.
- Sicherungsbänder täglich aus dem Serverraum in einen anderen Brandabschnitt in möglichst großer Entfernung sicher lagern.
- Funktionierende Gebäudetechnik ist Basis für den Wiederanlauf der IT.

- Die wichtigste und am meisten Nutzen bringende Entscheidung der Stadt war, für die Administration und Konzeption der kritischen Kernsysteme eine strategische Partnerschaft zu vereinbaren, die auch eine 24x7 Unterstützung bei systemkritischen Vorfällen beinhaltet.

Vielen Dank für Ihre Aufmerksamkeit

KISA

Agenda

1. kurzer Überblick zur Informationssicherheit
   - Was ist zu schützen?
   - Unsere Erfahrungen aus den Verwaltungen

2. Wenn das Worst-Case-Szenario Wirklichkeit wird – was tun im Katastrophenfall?
   (Albert Sturm, Stadt Straubing)

3. Unsere Unterstützungsleistungen für Sie

Unsere Unterstützungsleistungen für Sie

Stellung des Informationssicherheitsbeauftragten

- Verantwortung und Begleitung des Aufbaus der IT-Sicherheitskonzeption
  - Projektleitung und Steuerung
  - Orientierung an anerkannten Standards (BSI IT-Grundschutz bzw. Kompendium) aber Bedacht auf **Angemessenheit der Maßnahmen**
  - Dokumentation der einzelnen Schritte
  - „best practice“-Erfahrungen

- gemeinsame Erarbeitung geänderter oder neuen Dienstanweisungen /-vereinbarungen ➔ (IT)-„Compliance“
  - Erläuterung vor Personalrat und Leitungsebene
  - Vorstellung Kernaussagen gegenüber Mitarbeitern

Unsere Unterstützungsleistungen für Sie

Stellung des Informationssicherheitsbeauftragten

- Mitarbeiterschulungen und Sensibilisierungskampagnen
  - „Schlüssel für mehr Sicherheit“
  - individuelle Abstimmung der Themen und Teilnehmerkreise
  - Durchführung in Ihrer Verwaltung
  - nicht ausschließlich Vorträge
  - Beispielthemen: „Grundlagenschulung“, „E-Mails“, „Social Engineering“, uvm.

Unsere Unterstützungsleistungen für Sie

Stellung des Informationssicherheitsbeauftragten

- Unterstützung bei Sicherheitsvorfällen
- herstellerneutrale Hilfestellung und Prüfung bei Verfahrenseinführungen
- Empfehlungen für IT-Verantwortliche und Verwaltungsleitung
- regelmäßige Berichterstattung an die Verwaltungsleitung

KISA

Ohne ein **strategisches Gesamtkonzept** stehen die meisten IT-Sicherheitsmaßnahmen **„alleine“** da.

KISA

IT? Aber sicher!

KISA

Ihr Ansprechpartner

Marcus Kurth
Informationssicherheitsbeauftragter
+49 351 86652-441
marcus.kurth@kisa.it

Ich freue mich auf gute Gespräche mit Ihnen.