Donau-Universität Krems
Universität für Weiterbildung

Sicherheitskonferenz 2018 – Cyber-Sicherheitsvorfälle abwehren und erkennen - Worauf es in der Praxis ankommt

Ing. Thomas Mandl
Sr. Security Consultant, Owner
Cyber Defense Consulting Experts
eMail: thomas.mandl@cdce.at
web: www.cdce.at

CDCE Cyber Defense Consulting Experts

Version: 1.0 | Sprache: DE | Vertraulichkeitshinweis: UNRESTRICTED| TLP: WHITE

Agenda

- VORSTELLUNG
- EINSCHÄTZUNG DER LAGE – BEISPIEL RANSOMWARE
- PRAXISBEISPIELE
- LESSONS LEARNED
- CONCLUSIO

CDCE Cyber Defense Consulting Experts

WER BIN ICH?

Ing. Thomas Mandl

Seit 1988
- 8 Jahre **Alcatel Research** Center (Eisenbahnsicherungstechnik)
- Inhaber EU Patent EP 0 919 917 A3 (Sicherheitsbereich)

Seit 1995 IT und IT-Security Erfahrung
- Sr. Admin, später **IT Leiter bei Analog Devices Inc. VADC**
- Leitung **World Wide UNIX Security Teams** von Analog Devices

5 Jahre Anti-Virus Industrie (CTO von Ikarus Security Software)
- Aufbau des ersten österreichischen Frühwarnsystems **CIRCA**
- Publikationen bei Fachkonferenzen (VB, WTC, CMG-AE)

Lektor
- Seit 2003 Donau-Uni Krems, Seit 2006 FH Technikum Wien

Mitgliedschaften und Sonstiges
- Seit 2008 Vize-Vorsitzender des nationalen CERT.at Beirats
- Gründungsmitglied CSA, AIT Projektteam Schutz kritischer Infrastruktur
- SPG §55 Freigabe

Inhaber u. Sr. Security Consultant Cyber Defense Consulting Experts

CDCE Cyber Defense Consulting Experts

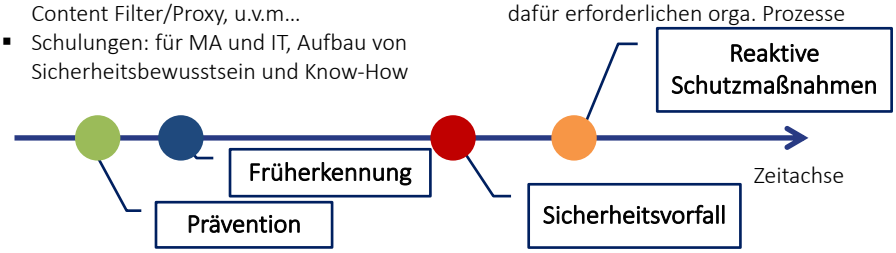
Wie unterstütze ich meine Klienten?

Vorbeugende Maßnahmen:

- IST Stand erheben (Audit/PenTest) : Sicherheitslücken finden, bevor Sie ein externer Angreifer findet.
- Sicherheitskonzept/Policy erstellen: Planung u. Umsetzung von tech. /orga. Vorgaben zum präventiven Schutz
- BCM/DR: Planung, Audit und Tests
- Setup und Wartung von Sicherheits-systemen: FW, IPS, WAF, Logging, Anti-Virus, Content Filter/Proxy, u.v.m…
- Schulungen: für MA und IT, Aufbau von Sicherheitsbewusstsein und Know-How

Schadensminimierung:

- Sofortmaßnahmen ergreifen: weiteren Datenabfluss verhindern
- Analyse: Was genau ist passiert, was wurden gestohlen/attackiert?
- Lessons Learned: Erstellen von vor-beugenden Schutzkonzepten damit Vorfall nicht nochmals passiert
- Verbesserung ihrer IT Sicherheit: Ausbau ihrer Schutzsysteme und der dafür erforderlichen orga. Prozesse



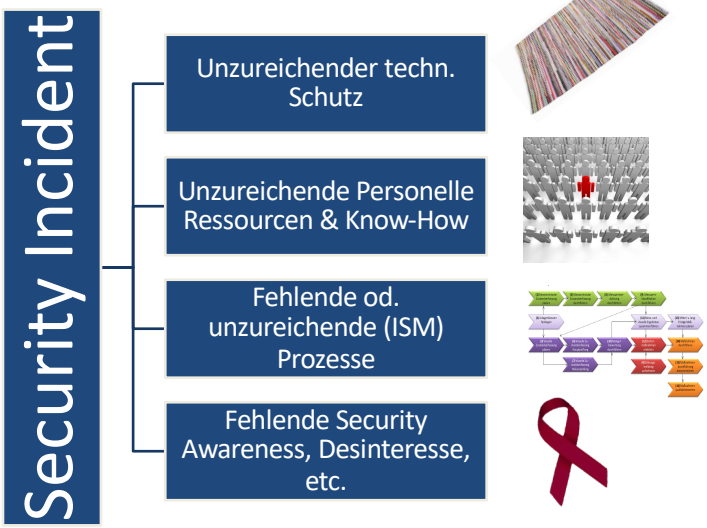
CDCE Cyber Defense Consulting Experts

EINSCHÄTZUNG DER LAGE AM BEISPIEL RANSOMWARE

Sicherheitsbewusstsein? Wer braucht das schon!

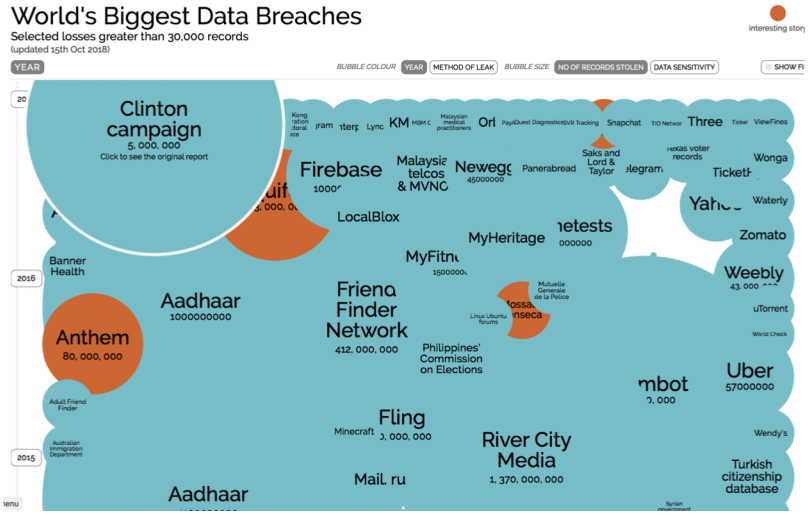
- Unternehmen verstehen die Komplexität von IT Lösungen nicht mehr bzw. sind nicht daran interessiert, diese zu verstehen solange es (irgendwie) funktioniert und günstig ist!
- Es fehlt an qualifiziertem IT Personal um Lösungen zu implementieren/dokumentieren
- Anwender werden nicht (mehr) eingeschult, es reicht aus, zu sagen, ich kenne mich in Office und im Internet aus.
- Es herrscht weiterhin der Irrglaube, dass *"das alles der ext. IT Dienstleister für uns macht"*, auch wenn ein Cyber-Angriff kommt, der hat "eh" vorgesorgt und kennt sich aus!

Gründe für Sicherheitsvorfälle

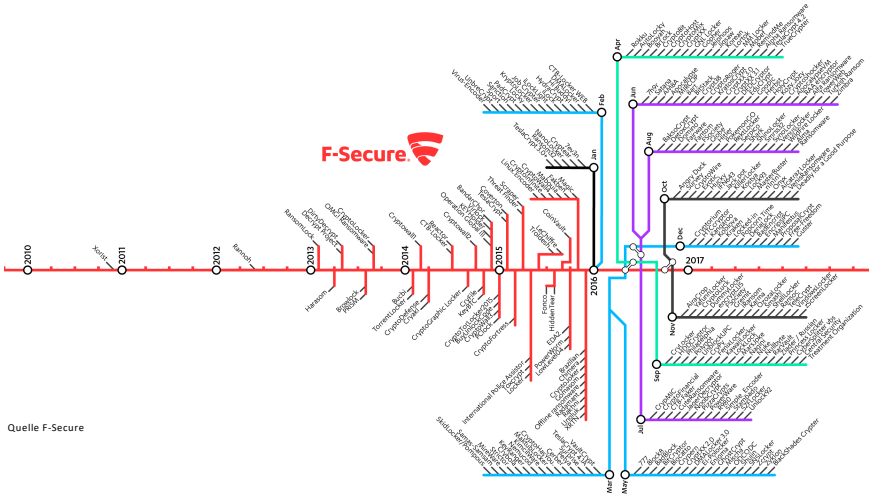


Wie ernst ist die Lage?

Quelle http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Anstieg von Ransomware-Familien



Quelle F-Secure

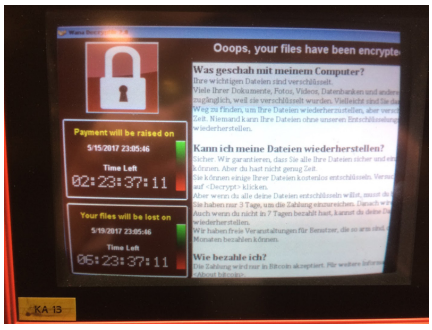
Beispiel Ransomware Attacke

Infektionsvektor: eMail mit „malicious“ Attachment

Prominente Opfer der „Wannacry“ Ransomware (Mai 2017)

Deutsche Bahn

Parkautomaten, Flughafen Berlin/Tegel



Quelle: https://heise.de/-3713426

Kritische Infrastruktur betroffen (12. Mai 2017)

In ganz England hat ein Kryptotrojaner am Freitag zahlreiche Krankenhäuser lahmgelegt. Und das ist offenbar nur die Spitze des Eisbergs einer globalen Welle von Infektionen mit Wana Decrypt0r 2.0 oder einfach WannaCry.

In ganz England sind Krankenhäuser offenbar Opfer eines Cyberangriffs, bei dem die Angreifer Computer mit Krypto-Trojanern sperren und nur gegen ein Lösegeld wieder freigeben wollen. Wie der *Guardian* berichtet, sind Krankenhausverbände im Süden und Norden Englands betroffen. Die IT ist dort entweder wegen des Trojaners nicht mehr benutzbar, oder weil Rechner aus Vorsicht heruntergefahren wurden. Teilweise werden Patienten gebeten, nicht in die Notaufnahmen zu kommen, sondern nur Notrufnummern zu wählen. Der Nationale Gesundheitsdienst hat inzwischen erklärt, dass der Angriff wohl nicht gezielt war, die IT-Abteilung eines Krankenhausverbunds in Liverpool spricht von einem "mutmaßlich nationalen Cyberangriff".

Quelle: https://heise.de/-3713235

CDCE Cyber Defense Consulting Experts

Wir dürfen der IT nicht die (ganze) Schuld geben

WannaCry: Mindestmaß an IT-Security hätte Chaos verhindert

28. Oktober 2017, 09:49 38 POSTINGS

Britischer Rechnungshof kritisiert Klinken in Großbritannien scharf

Die Ransomware WannaCry zählt wohl zu der schädlichsten Malware aller Zeiten. Über 230.000 Computer in 150 Ländern wurden befallen – nur durch Zufall konnte eine weitere Verbreitung gestoppt werden. In Großbritannien wurden sogar mehrere Krankenhäuser durch die Malware lahmgelegt. Der britische Rechnungshof hat sich mit WannaCry auseinandergesetzt und fällt ein vernichtendes Urteil: Die Kliniken hätten allesamt der Attacke entgehen können, wenn "grundlegende Praktiken zur IT-Sicherheit" beachtet worden wären.

Windows XP und fehlerhafte Firewalls

Konkret wurde in den Krankenhäusern auf ungepatchte und nicht mehr unterstützte Windows-Versionen genutzt, obwohl es bereits seit 2014 Pläne gab, auf ein neueres Betriebssystem umzusteigen. Zudem war die Firewall nicht richtig eingerichtet, was die Infizierung zusätzlich erleichterte. Am Tag der Attacke lief auf fünf Prozent der Rechner immer noch Windows XP, obwohl der Support für das System 2014 endete.

Chaos in Großbritannien nach Angriff

Tausende Sprechstunden und Operationen mussten im Zuge des Angriffs abgesagt und in fünf Regionen Patienten zu anderen Krankenhäusern gebracht werden. Verantwortliche waren für den Fall auch nicht vorbereitet – Absprachen zwischen den Klinken wurden zum Teil per WhatsApp erledigt. Der Schaden, der durch die Ransomware entstanden ist, konnte nicht beziffert werden. Lösegeld wurde zumindest keines bezahlt.

NSA-Hackingwerkzeuge für Attacke genutzt

Bei WannaCry nutzten Kriminelle entwischte NSA-Hackingwerkzeuge um ungepatchte Windows-PCs anzugreifen und dabei Dokumente zu verschlüsseln. Um diese Daten wieder freizugeben, wurde eine Lösegeld-Zahlung mittels Bitcoins eingefordert. Microsoft reagierte recht schnell und veröffentlichte einen Patch, um eine weitere Infektionswelle zu verhindern. Selbst Windows XP erhielt damals das Not-Update. (red, 27.10.2017)

https://derstandard.at/2000066778145/WannaCry-Mindestmass-an-IT-Security-haette-Chaos-verhindert

CDCE Cyber Defense Consulting Experts

Déjà vu - haben wir wirklich nichts dazugelernt?

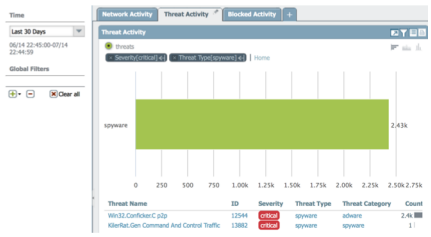
"Conficker"-Wurm legte Landesregierung und Spitäler in Kärnten lahm

12. Jänner 2009, 11:16 — 73 POSTINGS

Microsoft-Patch im November - Viele PC in betroffenen Krankenhäusern wieder am Netz

Nach einer Computervirenattacke ist am Montag die Routine in den Kärntner Landeskrankenhäusern wiederhergestellt worden. "Ein Großteil der rund 3.000 betroffenen PC ist bereits wieder am Netz", berichtete Rainer Harpf, IT-Leiter der Kärntner Krankenanstalten Betriebsgesellschaft (Kabeg) auf Anfrage. Auch in der Landesregierung ist der Betrieb wieder aufrecht. Rund 80 Prozent der Rechner seien wieder im Einsatz, erklärte Landesamtsdirektor Reinhard Sladko.

Quelle: https://derstandard.at/1231151587065/Conficker-Wurm-legte-Landesregierung-und-Spitaeler-in-Kaernten-lahm



Firewall Alerts ausgelöst durch Conficker IDS Signaturen im Sommer 2016

Verschärfung „Destroyware“ NotPetya (Juni 2017)

Millionenschaden bei drei Cyberangriffszielen in Österreich

29. Juni 2017, 13:08 — 148 POSTINGS

Weltweit haben Unternehmen mit Folgen zu kämpfen – Software tarnte sich als Erpressertrojaner, löschte aber Daten

Weltweit agierende Unternehmen haben nach wie vor mit den Folgen des massiven Cyberangriffs von Dienstag zu kämpfen. Dem Bundeskriminalamt (BK) wurden bisher drei Fälle von in Österreich betroffenen Firmen gemeldet. Der Schaden geht in die Millionen, hieß es am Donnerstag. Bei der Schadsoftware handelt es sich um eine Abwandlung der bekannten Ransomware "Petya", berichtete das BK.

Unternehmen und Behörden befallen

Die Schadsoftware hatte am Dienstag dutzende Unternehmen und Behörden in der Ukraine befallen und erfasste dann auch Firmen in Europa und den USA. Betroffen waren unter anderem der Nivea-Hersteller Beiersdorf, der US-Pharmakonzern Merck und der französische Glashersteller Saint-Gobain. Beim US-Logistikriesen Fed Ex war der weltweite Betrieb der Tochter TNT Express gestört. Der finanzielle Schaden könne "erheblich" sein, warnte Fed Ex am späten Mittwoch.

Bei der Reedereigruppe Maersk blieben Terminals in mehreren Häfen lahmgelegt. Die Maersk-Line-Reederei könne auch keine neuen Aufträge annehmen, weil das entsprechende Portal betroffen sei, sagte Manager Vincent Clerc dem Finanzdienst Bloomberg.

Unterschied zu bisheriger Ransomware: NotPetya ist ausschließlich auf Zerstörung aus, keine Möglichkeit durch Lösegeldzahlung die eigenen Daten wieder herzustellen.

https://derstandard.at/2000060537928/Millionenschaden-bei-drei-Cyberattacke-Zielen-in-Oesterreich

Verluste durch “Destroyware” weltweit sehr hoch

NotPetya: Maersk erwartet bis zu 300 Millionen Dollar Verlust

16.08.2017 18:08 Uhr – Fabian A. Scherschel vorlesen

Die Gunvor Mærsk der Maersk Line mit Kurs auf den Hamburger Hafen. (Bild: Bernhard Fuchs, CC BY 2.0)

Containerterminals standen still, Schiffe konnten weder gelöscht noch beladen werden: Mehrere Wochen hielt der Trojaner den dänischen Mega-Konzern Maersk in Atem. Die Reederei Maersk Line und der Hafenbetreiber APM Terminals wurden schwer getroffen.
https://heise.de/-3804688

Nach NotPetya-Angriff: Weltkonzern Maersk arbeitete zehn Tage lang analog

26.01.2018 15:00 Uhr – Fabian A. Scherschel vorlesen

Jim Hagemann Snabe, der Vorsitzende des Weltkonzerns A.P. Møller-Maersk, erzählt in Davos sichtlich bewegt von den Erfahrungen seiner Firma mit NotPetya. (Bild: YouTube)

Wenn die Computer ausfallen, muss die Arbeit im Zweifel wieder auf die altmodische Art erledigt werden: mit Papier und Stift.

Das dänische Industrie-Konglomerat Maersk hat wie kein anderes Unternehmen unter dem vermeintlichen Ransomware-Angriff der Schadsoftware NotPetya gelitten. Nach konservativen Schätzungen kostete der beispiellose Hacker-Angriff im Juni 2017 das Unternehmen mehrere hunderte Millionen Dollar. Nun hat der Vorsitzende der Firma in einer Diskussionsrunde auf dem Weltwirtschaftsforum in Davos zum ersten Mal öffentlich darüber gesprochen, wie sich der Angriff aus Sicht der Firma im Detail darstellte. Demnach musste Maersks IT-Abteilung innerhalb von zehn Tagen große Teile der Computer-Infrastruktur neu aufsetzen – Mitarbeiter waren unterdessen gezwungen, komplett analog zu arbeiten.
https://www.heise.de/newsticker/meldung/Nach-NotPetya-Angriff-Weltkonzern-Maersk-arbeitete-zehn-Tage-lang-analog-3952112.html

CDCE Cyber Defense Consulting Experts

Das Know-How
eines Unternehmens und
die Arbeit von Jahrzehnten kann
innerhalb von Sekunden
durch eine unbedachte Handlung
zerstört werden
(Ransomware, Destroyware)!

CDCE Cyber Defense Consulting Experts

Unterschiede Ransomware und Destroyware

Zitat IT-Mgnt nach friendly Audit: *“Das war uns so nicht bewusst, dagegen haben wir nicht vorgesorgt”!*

Klassische Ransomware | Destroyware (NotPetya)

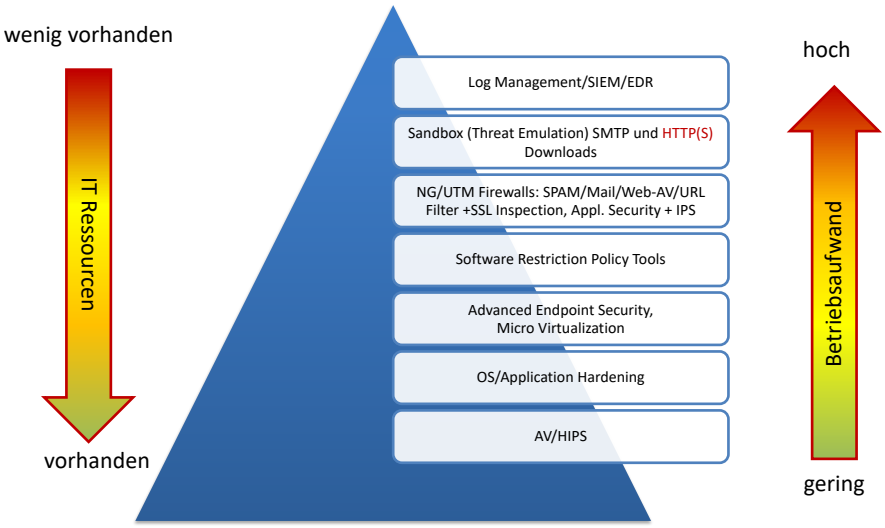
Notfallvorsorgepläne werden daher umso wichtiger!

CDCE Cyber Defense Consulting Experts

PRAXISBEISPIELE

LESSONS LEARNED

Wie reagieren wir typischerweise darauf?



CDCE Cyber Defense Consulting Experts

Was kann helfen?

Security Awareness der Mitarbeiter & Mgnt.

IT-Security (techn. Lösungen z.B. Virus Scanner, Firewalls, …)

Information Security (orga. Lösungen wie z.B. Policies, Guidelines, …)

Unternehmenssicherheit (Summe d. Maßnahmen, RM, BIA, BCM…) = **ISMS**

CDCE Cyber Defense Consulting Experts

Security Awareness auf- bzw. ausbauen

Awareness ist wichtig, wird aber nicht alle Probleme lösen!

- IT Grundlagen zur Früherkennung von Bedrohungen vermitteln
- Ansprechperson(en) für IT und InfoSec definieren. Sind Anlaufstelle für Sicherheitsfragen und übernehmen interne Kontrollfunktionen (Park Sheriff) kombiniert mit Belohnungen (*positive incentives*)
- Beispiel: MA in Buchhaltung verhindert CEO Fraud, weil „mitgedacht“ wurde –> Belohnung!
- Betriebsrat & Innenrevision/Compliance Abteilung einbinden

Vorbildwirkung des Managements nicht vergessen

- George Orwell „Animal Farm“: Alle Tiere sind gleich. Aber manche sind gleicher als die anderen.“

CDCE Cyber Defense Consulting Experts

Organisatorische Voraussetzungen schaffen

Dokumentationspflicht ernst nehmen

- Interne IT aber auch externe IT Dienstleister, Zeit für Dokumentation bereitstellen (Kosten berücksichtigen)

Requirements Management

- Anforderungen an Sicherheitslösungen definieren

ISMS Prozesse leben und nicht nur Papier produzieren

- Patch & Vuln. Management kann „Attack Surface“ reduzieren und hätte so manche erfolgreiche Cyber-Attacke bereits vereitelt

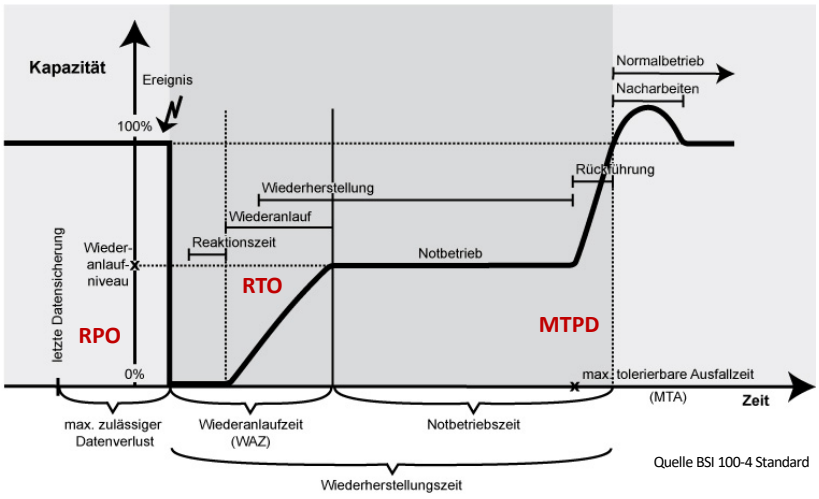
Business Continuity Management (BCM) etablieren

- BIA & Kennzahlen definieren (RTO, RPO, MTDT)
- Notfallplan vorbereiten & Notfallvorsorge + Notfallkommunikation planen und umsetzen

DSGVO Meldeprozesse nicht vergessen

CDCE Cyber Defense Consulting Experts

Notfallablauf nach BSI 100-4 Standard



Quelle BSI 100-4 Standard

CDCE Cyber Defense Consulting Experts

Realität vs. Best Current Practice

Wer hat (rudimentäre) Notfallplanung bzw. IR-Planung?

- Sind BCM Parameter (RTO, RPO, MTDT) für essentielle Geschäftsprozesse definiert?
- Sind Geschäftsprozesse überhaupt definiert/dokumentiert (KMU?)
- Sind Zuständigkeiten für Vorsorge klar geregelt?
- Gibt es Anweisungen für den Incident-Response (IR) Fall?

IT ist oft treibende Kraft hinter Notfallplanung, aber

- IT Infrastruktur ist historisch gewachsen & Zitate Mgnt:
  - *Dann lagern wir halt alles, aus, soll sich ein externer Dienstleister darum kümmern!*
  - *Dann gehen wir halt in die Cloud, da funktioniert alles zuverlässiger!*
  - *Warum hat die IT das nicht im Griff? Ich dachte, das ist alles geregelt und wir überstehen einen Notfall?*
  - *Bisher ist auch noch nichts passiert, warum brauchen wir einen Notfallplan?*

CDCE Cyber Defense Consulting Experts

Kontrollfragen und Best Current Practice

Wie zuverlässig ist meine Datensicherung?

- Wer kontrolliert, ob Datensicherung tatsächlich zuverlässig funktioniert (oft kein proaktiver Backup/Recovery Test) → Man verlässt sich auf externen Dienstleister, der wird das schon machen
- Praxisbeispiel: Dateipfade > 256 Ch. sorgen oft für Probleme bei Sicherung/Wiederherstellung
- Oft nur Systemsicherung kaum Langzeitdatenarchivierung
- Verfügbarkeit von Backups im KMU Bereich zw. 14 – 30 Tage → Risiko Long Termin Ransomware Angriffe
- Max. Dauer der Datenwiederherstellung oft unbekannt
- Lassen Sie ihre IT auditieren (friendly Audit)

CDCE Cyber Defense Consulting Experts

Kontrollfragen und Best Current Practice

Werden Security Kennzahlen (KPIs) erhoben?

- Werden Lessons Learned aus KPIs abgeleitet?

Verschärfung von Sicherheitseinstellungen unerwünscht

- Striktes URL oder File Blocking unerwünscht od. unmöglich (blockiert etablierte Workflows)
- Zitat Mgnt.: *„MA müssen so ungestört wie möglich arbeiten können, Produktivität geht vor Komfort und vor Sicherheit!“*

Falsche bzw. nicht aufeinander abgestimmte Technologien im Einsatz

- Selten “echtes” Requirements Management (historisch gewachsene IT (Sicherheits)Landschaft

CDCE Cyber Defense Consulting Experts

Was können wir von der Medizin lernen?

- Je früher wir eine schlimme Krankheit entdecken, umso eher besteht Heilungschance
- Vorsorgeuntersuchungen = friendly Audit (Prävention) wichtig, aber auch richtige Reaktion bei Ausbrauch einer Krankheit (z.B. medizinische Notfallversorgung)
- Ohne genaue Analyse der Begleitumstände und Rahmenparameter (Blutbild, MRT/CT, …) einer Krankheit, keine genaue Diagnose
- Security Incidents “trainieren” und Verhaltensregeln aufstellen (vgl. med. Triage bei Notarzt)
- Orga. Prozesse schaffen um Technik & Mensch zu unterstützen
- Nicht alles an externe DL auslagern, Kernkompetenzen im Haus lassen → Know-How selber beginnen aufzubauen, eigenes IT Personal kennt seine Systeme am Besten

CDCE Cyber Defense Consulting Experts

Incident Response Prozesse etablieren

- Der Prozess war vergleichseweise leicht zu entwerfen, die IT aber soweit zu bekommen, dass sie die erforderlichen Daten innerhalb einer angemessenen Zeit (72 Std.) liefern kann ist viel komplexer und kurzfristig kaum zu schaffen!
- Kaum eine IT Abteilung ist dafür bereits aufgestellt!
- Hersteller liefern teilweise nicht die erforderlichen Informationen, Zeitdruck, Ressourcenmangel bei IT, Frustration, das man nicht angehört wird, usw…
- Kosten professioneller Lösungen schrecken ab (KMU Budget)
- Outsourcing ohne Konzept und Kontrolle, der externe DL wird das schon machen!
- Best Current Practices gibt es schon lange (BSI Grundschutz, ISO27001, österreichisches Sicherheitshandbuch!

CDCE Cyber Defense Consulting Experts

CONCLUSIO

Conclusio

Das Ziel ist eine
Reduktion von Cyber-Risiken
und die
Erhöhung der
Resilienz Ihres
Unternehmens

CDCE Cyber Defense Consulting Experts

Vielen Dank für Ihre Aufmerksamkeit

Q & A

CDCE Cyber Defense Consulting Experts

Cyber Defense Consulting Experts e.U.

eMail: office@cdce.at
Internet: www.cdce.at

Ing. Thomas Mandl
Sr. Security Consultant & Owner
thomas.mandl@cdce.at
+43-664/392-16-68