THE SPIR.IT OF EXCELLENCE

iT-Sicherheit zu Zeiten von Corona: Erfahrungsbericht aus dem 'new normal'

Vortrag im Rahmen des iT-Sicherheitstages NRW 2020

Tobias Rademann

2. Dezember 2020

Agenda

1. Auswirkungen von Corona auf die iT-Sicherheit
2. Konsequenzen & Lösungsansätze
3. Résumée: Das 'new normal'

Ihr Nutzen

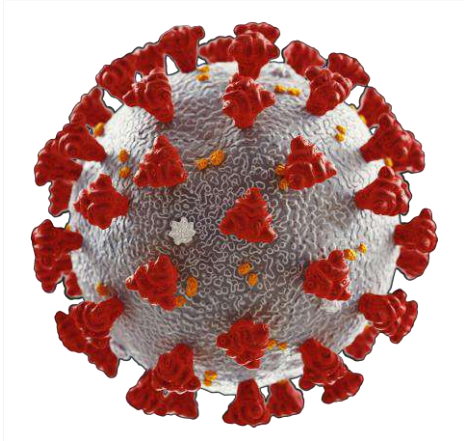
- ✓Sensibilisierung für die Auswirkungen von Corona
- ✓Lösungsansätze für *effektives* Vorgehen
- ✓Anforderungen an iT-Sicherheit nach Corona

Kurzprofil: R.iT GmbH

- **Fokus:** iT-Unternehmensberatung für die Digitale Transformation
- **Kernthemen:** Digitalisierungsberatung
  > (Digital) Strategie
  > Geschäftsprozessautomatisierung
  > angewandte iT-Sicherheit
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Standorte** Zentrale: Bochum
  Region Nord: Bad Schwartau
- **Zertifizierung:** BMWi-autorisiert für > iT-Sicherheit *und*
  > digitale Geschäftsprozesse
  EFQM: Recognized for **Digital Excellence*****

Auswirkungen von Corona auf die iT-Sicherheit

Corona –
ein *realer* Virus bedroht die *digitale* Infrastruktur



steigende Bedrohungslage durch Corona

Gründe:

1. verteiltes Arbeiten
2. steigende Verunsicherung
3. 'mehr mit weniger'

steigende Bedrohungslage durch Corona

Gründe:

1. **verteiltes Arbeiten**
   - **massiv steigende Komplexität**
     → iT-Sicherheitsanforderungen und -aufgaben nehmen rasant zu
   - **schnelle Veränderungen, oft ohne vorhandenes Konzept**
     → reaktives Vorgehen, aufwendige Nachbesserungen
   - **fehlender Austausch mit Kolleginnen und Kollegen**
     → Menschen machen Fehler, weil sie Dinge nicht absprechen / klären können

➔ größere Angriffsfläche = Basis für (erheblich) **größeres Schadenpotential**

➔ mehr Lücken = Basis für (erheblich) **gestiegene Verwundbarkeit**

steigende Bedrohungslage durch Corona

Gründe:

1. *verteiltes Arbeiten* ✓
2. **steigende Verunsicherung**
   - **Angst vor Corona**
     → Menschen suchen online nach Informationen
   - **zunehmende Isolation**
     → Menschen suchen online nach Kontakten / Kommunikation
   - **zunehmender Druck**
     → Menschen machen mehr Fehler

➔ Basis für Phishing Angriffe, CEO-Fraud & Trojaner (Ransomware)

➔ Risikofaktor Mensch nimmt zu = Basis für (erheblich) **gestiegene Verwundbarkeit**

steigende Bedrohungslage durch Corona

Gründe:

1. *verteiltes Arbeiten* ✓
2. *steigende Verunsicherung* ✓
3. **'mehr mit weniger'**
   - **strategische Ebene:** Fokus auf Arbeitsfähigkeit, ~~nicht auf iT-Sicherheit~~
   - **operative Ebene:** weniger Personal verfügbar für iT-Sicherheit
     komplexere Prozesse *(s.o., verteiltes Arbeiten)*
   - **finanzielle Ebene:** weniger Geld verfügbar

→ iT-Sicherheitsmaßnahmen stagnieren bzw. fallen bei steigenden Anforderungen

➔ mehr Lücken = Basis für (erheblich) **gestiegene Verwundbarkeit**

➔ größere Angriffsfläche = Basis für (erheblich) **größeres Schadenpotential**

iT-Sicherheit und Corona

gestiegene Verwundbarkeit + größeres Schadenpotential

Konsequenzen & Lösungsansätze

Konsequenzen

Was hat sich geändert?

→ Das ist nun wirklich nichts Neues…

Konsequenzen

Was hat sich geändert?

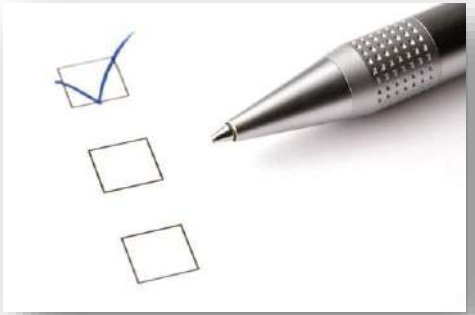
aber:

- zunehmende Verunsicherung – gerade bei Geschäftsführung & Vorstand
- Notwendigkeit der umfangreichen Nachbesserung
- Herausforderung, 'mehr mit weniger' erreichen zu müssen

Konsequenzen

Was hat sich geändert?

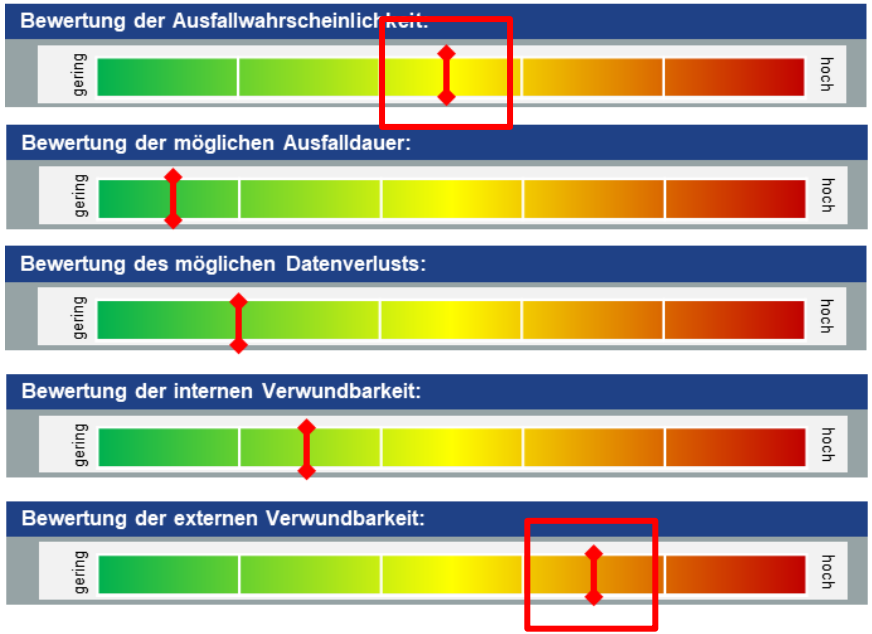
1.)
Entscheider suchen
Orientierung & Überblick



2.)
Einschätzung
Handlungsbedarf

3.)
angemessene **Priorisierung**
ganzheitliches Konzept

iT-Risk Assessment: Status Quo Übersicht



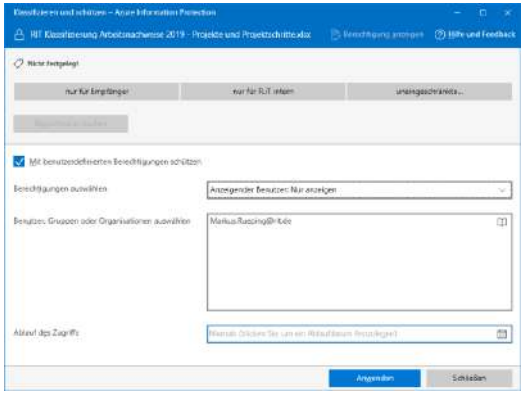
iT-Risk Assessment: Handlungsempfehlungen

iT-Risk Assessment durch die R.iT GmbH (September 2020)
Handlungsempfehlungen

Reihenfolge	empfohlene Maßnahme	Umsetzungsdetails	(Risiko-)Bereich	Priorisierung / Wichtigkeit	Priorisierung: Dringlichkeit
1	W-LAN restrukturieren	- Gäste W-Lan vom Produktivnetz trennen - Internes Netzwerk erstellen - Smartphone Netzwerk	externe Verwundbarkeit	wichtig	dringend
2	Ausfallrisiko der USVen reduzieren	- Batterien der zwei älteren USVen austauschen	Ausfallwahrscheinlichkeit	wichtig	dringend
3	Webseite rechtskonform ausgestalten	-Cookie-Banner aktualisieren	interne Verwundbarkeit	wichtig	dringend
4	Hyper-V Replikation anpassen	- Replikationszyklen von DB- und Exchange-Server verringern - fehlende Server replizieren (wenn erforderlich)	Datenverlust	wichtig	dringend
5	Internes anonymes Versenden von E-Mails unterbinden	- Versand ohne Authentifizierung deaktivieren - Drucker falls notwendig umstellen - [redacted] mit Authentifizierung umstellen - Skripte welche E-Mails versenden anpassen	externe Verwundbarkeit	wichtig	dringend
6	Kennwortrichtlinien und Kennwortänderungen	- Kennwortrichtlinie definieren und umsetzten - Administratorkennwörter verstärken - Einrichtung eines gemeinsam nutzbaren Passwortmanagement-Tools für die Administratoren für die Verwaltung generischer Kennwörter - Standard Kennwörter der IP Telefone ändern	externe Verwundbarkeit	wichtig	dringend
7	[redacted] absichern	- [redacted] Anmeldung auf AD Ebene - Standard Kennwörter ändern (Bspw [redacted] - SQL Authentifizierung abstellen / Benutzer bereinigen	interne Verwundbarkeit	wichtig	dringend
8	Strategische Grundlagen für Notfallmanagement herstellen	- Erstellung eines Datensicherungskonzepts - Erstellung eines Notfallplan - Einführung von jährlichen Disaster Recoveries	Ausfalldauer	wichtig	nicht dringend
9	Interne Netzwerke abtrenne und absichern	- Server, Clients, Drucker, Telefone, Hausautomatisierung und WLANs in separate Netzwerke auftoilen - NAC Lösung implementieren	externe Verwundbarkeit	wichtig	nicht dringend
10	Komplettes Refactoring aller Intranet-Komponenten in einer modernen und sicheren Entwicklungssprache	- ASP Skripte abschaffen und durch moderne Plattformlösung ersetzten, die keine Kennwörter und Benutzernamen enthalten - Quellcode Verwaltung einführen und mit dem IIS verknüpfen	externe Verwundbarkeit	wichtig	nicht dringend
11	Firewall-Regelwerk überarbeiten	- DNS auf die Domain Controller beschränken - Internet des Backupnetztes beschränken - SharePoint für außen unzugänglich machen	interne Verwundbarkeit	nicht wichtig	dringend
12	Geräteverschlüsselung implementieren	- Verschlüsselung aller Notebooks und Computer	Datenverlust	nicht wichtig	dringend
13	Patchmanagement für Hardwarekomponenten etablieren	- Mechanismus für regelmäßig mit Updates des Backends	Ausfallwahrscheinlichkeit	nicht wichtig	dringend

konkrete Schritte, *die fast immer passen…*

- **Angriffsfläche verkleinern**
  - Unterstützung der Mitarbeitenden: Sensibilisierung und Support
  - Sensibilisierung der Führungskräfte für neue Aufgabe: Überwachung und Durchsetzung der iT-Sicherheitsrichtlinien
  - sichere und skalierbare Verbindungen (SDP statt VPN, MFA)
- **Schadenrisiko reduzieren**
  - Disaster Recovery (Business Continuity I)
  - sichere Daten (Verschlüsselung; cloud: Azure Information Protection)
  - 'mobil verfügbarer' Notfallplan (Business Continuity II)



Résumée: Das 'new normal'
– gerade im Bereich der iT-Sicherheit

Résumée

Was ist das 'new normal'?

➔ **nicht**: ~~MO (Mobile Office), Abstand oder Maskenpflicht~~

Résumée

Was ist das 'new normal'?

➔ Corona als wertvolles Beispiel für massive **Veränderungsprozesse** und deren **Konsequenzen**

Résumée

Digitalisierung oder besser 'Digitale *Transformation*':

= **massive Veränderungen** infolge des exponentiellen Fortschritts im Bereich der Leistungsfähigkeit moderner iT

➔ **new normal**: **massive Veränderungen** in der (Arbeits-)welt

Résumée

'new normal'

- zentrale Anforderung: Fähigkeit, sich **schnell anzupassen**
- zentrale Anforderung iT-Sicherheit: Fähigkeit, sich **schnell anzupassen**, **ohne das Risiko (ungewollt) zu erhöhen**

- Corona hat auch gezeigt: Anpassungsfähigkeit ist viel mehr als Technik


strategisch


organisatorisch


iT-bezogen

→ gilt auch für iT-Sicherheit: flexibles, ganzheitliches Konzept, ~~reaktives Stückwerk~~

let's shape a **safe** future – *together*!

offene Fragen / Diskussion

Vielen Dank für
Ihre Zeit und Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:

THE SPIR.IT OF EXCELLENCE

Tobias Rademann, M.A.
R.iT GmbH • www.RiT.de
Zentrale: Amtmann-Ibing-Str. 10, 44805 Bochum
Tel.: (0234) 43 88 00-0, Fax: -29
NL Nord: Tremskamp 5, 23611 Bad Schwartau
Tel.: (0451) 203 68-500, Fax: -499
eMail: Tobias.Rademann@RiT.de