Backup Risk Assessment

- Abschottung der Backup Umgebung(en) gegen Ransomware -

UC ADVISORY dignum®

Vorteile & Alleinstellung

UC-Advisory & dignum verknüpfen die hohen Security-Kompetenzen und das tiefe Know-How aus der Infrastruktur miteinander. Hierdurch sind deutliche Mehrwerte in der Beratung sichtbar.

Folgende Vorteile erreichen Sie mit unserem „Backup Risk Assessment“:

- Transparenz / Darstellung der Risiken in Ihrer Backup Umgebung
- Konkrete Handlungsempfehlungen zur proaktiven Risikominimierung
- Erhöhung der Sicherheit für das Gesamtunternehmen
- Erhöhung der Resilienz der Backup Umgebung gegenüber Ransomware Angriff en
- Stärkung der eigenen Handlungs- & Reaktionsfähigkeiten

Widerstandskraft

Ein Scheitern ist vorprogrammiert, wenn ich das Backup mit denselben Methoden & Prozessen absichere, wie ich es mit dem restlichen Unternehmensnetzwerk getan habe!

- Die Sicherheitsanforderungen an die Backup Infrastruktur sollten in unseren Augen höher sein, als für den Rest der Unternehmens-Netzwerke
- Wir müssen die **Backup Kill Chain brechen**
- Auch bei der Kompromittierung von Teilbereichen müssen die Restore Fähigkeiten erhalten bleiben
- Das Ziel aus der Zusammenarbeit mit uns lautet, dass Sie nach einer Sicherheitsüberprüfung oder einem Ransomware Befall sagen können:

„Ja, Server X und System Y mag betroffen sein, meinetwegen das ganze Netzwerk,

ABER

- *wir sind vorbereitet,*
- *wir haben eine funktionale Backup Umgebung,*
- *wir sind umfassend Restore fähig,*
- **das Backup ist sicher!“**

Risiko & Angriff

- Ransomware Attacken auf Unternehmen, Verwaltungen und Einrichtungen nehmen drastisch zu
- Kosten zur Bewältigung verdoppeln sich nahezu jährlich
- ø-Gesamtkosten weltweit steigen auf **203 Mio. US-Dollar pro Tag**
- Hacker gehen inzwischen gezielter und mit höherem Aufwand vor
- Security-Experten erwarten noch komplexere Angriff e mit noch höherem Zerstörungs-Potential in der nahen Zukunft
- **Backup ist immer primäres Ziel** bei einer Ransomware Attacke
- Backup = „Last Line of Defense“ - erst ohne funktionierendes Backup ist man wirklich gezwungen den Erpresser zu bezahlen

Herausforderungen

- Angreifer halten sich i.d.R. länger im Unternehmen auf (Lateral Movement)
- Angriff e auf das Backup erfolgen aus dem internen Netz heraus
- Backup benötigt grundsätzlich offene Schnittstellen und Ports … und kann ohne weitreichende Berechtigungen nicht funktionieren
- Komfort und einfache Bedienbarkeit stehen im Widerspruch zur Sicherheit
- Wiederherstellbarkeit muss schnell gegeben sein, dies kann klassische (passiv / Tape) und moderne (Cloud) Ansätze erschweren bzw. verhindern
- Kosten- und Zeitdruck in der IT insgesamt und in der Rechenzentrums-Infrastruktur im Besonderen weichen die Sicherheitsanforderungen auf und drängen Tests sowie Dokumentationen in den Hintergrund
- Security-Spezialisten planen, reden und denken anders als die Kollegen aus der Infrastruktur - das muss Teil der Betrachtung sein
- Sicherheitsbetrachtungen sind kein einmaliges, abgeschlossenes Ereignis, sondern ein permanenter Prozess

Ansprechpartner: **Achim Kapitz**
Spezialist für Backup, Recovery und Ransomware Resiliency
Gründer der „NetBackup Usergruppe“ & von „KiSS, das Keepit-Forum“
Mobil: +49 - 160 - 90 63 8686
eMail: achim.kapitz@dignum.de