Backup Risk Assessment
- Isolating Backup Environment(s) from Ransomware

UC ADVISORY dignum®

Advantages & Unique Position

UC-Advisory & dignum combine extensive security expertise with deep infrastructure know-how. This generates clear added value in our consulting services.

With our „Backup Risk Assessment“ you gain the following benefits:
- Transparency / visualization of risks in your backup environment
- Precis recommendations for proactive risk minimization
- Increasing security for the entire company
- Increasing the resilience of the backup environment against ransomware attacks
- Strengthening one's own capacity for action and reaction

Resilience

Failure is inevitable if you secure the backup using the same methods and processes you used for the rest of the corporate network!

- From our point of view, the security requirements for the backup infrastructure should be higher than those for the rest of the corporate networks
- We must **break** the **backup kill chain**
- Restoration capabilities must be maintained even if only some areas are affected
- The objective of working with us is for you to be able to say, following a security assessment or a ransomware attack:

„Yes, server X and system Y may be affected, or even the entire network“

BUT
- *we are prepared,*
- *we have a functional backup environment,*
- *we are fully capable of restoring,*
- ***the backup is guaranteed! “***

Risk & Attack

- Ransomware attacks on companies, administrations and institutions have spiked significantly
- Coping costs nearly double every year
- Average total costs rise to **203 million USD per day** worldwide
- Nowadays hackers are increasingly precise in their targeting and are dedicating substantially greater resources
- Security professionals forecast a surge of highly sophisticated cyberattacks capable of inflicting unprecedented systemic damage
- Modern ransomware operators **systematically** target **backup repositories**
- Backup = „Last line of defense“ - without a working backup are you truly forced to pay the extortionist

Challenges

- Attackers generally remain inside the company for longer periods (lateral movement)
- Attacks on the backup originate from the internal network
- Fundamentally, backups require open interfaces and ports ... and cannot function without extensive permissions
- Good and easy usability conflict with security
- Recoverability must be achievable quickly; this can complicate or even rule out traditional (passive/tape) and modern (cloud) approaches
- Time and budget pressures are compromising security standards, relegating essential testing and documentation to an afterthought
- Security specialists plan, communicate, and think differently than their colleagues in infrastructure - and this must be taken into consideration
- Security considerations are not a single, completed event, but an ongoing process

Contact us:

Achim Kapitz
Specialist for Backup, Recovery and Ransomware Resiliency
Founder of „NetBackup User Group“ & „KiSS, the Keepit-Forum“
Mobile: +49 -160 -90 63 8686
eMail: achim.kapitz@dignum.co.za