Neem deze security-maatregelen bij data-storage

18 FEBRUARI 2016 09:26 | BIRGIT BUNT

Er zijn nogal wat security-maatregelen die moeten worden genomen bij data-storage en de exposanten van de drie gecombineerde ict-vakbeurzen Infosecurity.be, Storage Expo en The Tooling Event weten hier alles van. In dit artikel geven ze alvast een voorproefje van de tips en informatie die zij u kunnen geven tijdens de vakbeurzen op 23 en 24 maart in Brussels Expo.

Welke security-maatregelen organisaties moeten nemen bij data-storage is erg afhankelijk van de situatie waar de organisatie zich in bevindt, zegt Martijn van Lom, general Manager bij Kaspersky Lab Benelux. Over het algemeen moet je volgens hem denken aan back-ups, wie heeft er toegang tot de data, is de data altijd bereikbaar, is de data versleuteld, et cetera. Ook Peter Magez, country manager Belux bij Sophos, meent dat er met veel domeinen rekening moet worden gehouden bij databeveiliging. ‘Enerzijds is er informatie die in-house wordt bewaard, maar er wordt binnen bedrijven ook steeds meer gebruik gemaakt van cloudstorage-systemen en externe media om data te delen. En dan hebben we het nog niet eens over mails die worden gestuurd met gevoelige data en bijvoorbeeld ‘per ongeluk’ worden doorgestuurd naar iemand die er niets mee te maken heeft.

Datamanagement

Volgens Kristof Lossie, security engineer bij Check Point Belux, moet data storage starten met goed datamanagement. ‘Dit houdt in een goede classificatie van data, welke data zijn belangrijk, welke zijn confidentieel en wie heeft de toegangsrechten? Deze classificatie bepaalt

grotendeels welke security-maatregelen er moeten getroffen worden voor welk type data.' Prodata Systems meent dat de data die als 'belangrijk' is geclassificeerd, vervolgens veilig moet worden bewaard in een omgeving die onvoorziene uitval van it-onderdelen en volledige datacenters opvangt. 'In functie van de behoefte (rto-rpo), kan dit relatief eenvoudig of vrij complex worden. Belangrijk is ook dat ervoor gezorgd wordt dat de data enkel gebruikt wordt door bevoegden en niet misbruikt kan worden door externen. Binnen de datacenters lukt dat meestal wel, maar denk ook aan de data op mobiele apparaten en de data die al dan niet bewust verstuurd wordt door eigen personeel.'

Fysieke beveiliging

Daarnaast moet er volgens Lossie ook rekening worden gehouden met de fysieke beveiliging van data-storage en de lifecycle van het medium. Mark Adriaenssens, oprichter van Out Of Use, voegt daar aan toe dat veel bedrijven in hun Data Security Policy vergeten aan te geven wat er moet gebeuren met data nadat apparatuur waar die op opgeslagen staan wordt afgeschreven en vervangen.

Encryptie en meer

Lossie meent dat encryptie hier een belangrijke en veel te weinig geïmplementeerde technologie is. Ook Rob Huikeshoven en Benjamin Budt, security experten bij Infradata, zien het belang in van encryptie. Daarnaast noemen zij als belangrijke security-maatregelen onder andere plugins om malware en virussen te detecteren op storage niveau; deduplicatie; back-ups en de zesmaandelijkse test daarvan voor kritische bedrijfsomgeving; Identity access management op systemen die toegang tot storage hebben. Jochen Bonne, director Azlan Belgium bij Tech Data, meen ten slotte dat privacy en availability twee belangrijke thema's bij databeveiliging zijn.

Ultieme tips

- Laat uw oude apparatuur ophalen door een gecertificeerd bedrijf (ISO9001/ISO14001) dat u een attest kan bezorgen van datavernietiging (DIN66399 klasse H3 of H5, of gecertificeerde software datavernietiging in geval van hergebruik van de oude apparatuur.
- Ga ervan uit dat het een kwestie van tijd is voor er een disaster gebeurt op vlak van data.
- Wees kritisch op de gekozen oplossing en neem additionele maatregelen om de beveiliging op meerdere niveaus te verbeteren. Doe ook intensief onderzoek naar derden die u inschakelt om zorg te dragen voor de data storage van uw bedrijf.
- Gebruik goede encryptie en zorg voor een enterprise mobility management-oplossing.

- Encryptie blijft de belangrijkste tip.
- Blus geen brandjes, maar maak een goede analyse van wat je hebt en wat je wil bereiken, rekening houdend met de zaken die uw bedrijf nodig heeft om verder te groeien.
- Security is geen lineair gegeven meer. Organisaties moeten daarom verschillende lagen van bescherming aanbrengen om de beveiliging zo optimaal mogelijk te krijgen.