TechData A TD SYNNEX Company

VERITAS

Weerbaar worden voor Ransomware bedreigingen?

Neem de controle terug, met Veritas Backup Exec®

Afgelopen jaar is er een enorme groei geweest in aanvallen op organisaties, overheden en publieke diensten, zowel groot als klein en wereldwijd. Ze hebben onder andere geresulteerd in tekorten aan gas, ontregelde zorgsystemen, gesloten winkels, in scholen die dicht moesten en in stilgelegde fabrieken.

40%
Heeft een cyberaanval gehad

45%
Van slachtoffers van een aanval hebben klantdata verloren

65%
Heeft omzetverlies geleden

53%
Heeft merk- en reputatieschade geleden

25%
Moest tijdelijk of geheel stoppen met de business

De hackers zijn gemotiveerd

Slachtoffers betaalden tot **$50,000** aan kosten om te herstellen, of zij nu wel of geen losgeld betaalden.

Het gemiddelde losgeld dat werd verlangd steeg met 43% in 2021, met een gemiddelde betaling van 58% naar

$78,398

Criminele organisatie	Verantwoordelijk voor...
REvil Gemiddeld US 2,5 mio per aanval gescoord	* JBS (US 1,1 mio) * Kadeya die duizenden kleinere organisaties heeft geraakt en tienduizenden systemen heeft platgelegd (zij vroegen US 70mio voor een universele decryptie key)
Conti Maken geregeld miljoenen buit	* ExaGrid aanval (US 2,6mio) * Aanval op Iers zorgsysteem * Aanvallen op 400+ organisaties wereldwijd waarvan 290 US organisaties
Maze Maken gemiddeld $ 420K buit per aanval	* Aanval op City of Pensacola, Florida * Aanval op Southwire
DarkSide Ontvangen miljoenen aan losgeld	* Aanval op Colonial Pipeline (US 4,4mio)
Lazarus Group Hebben naar verwachting miljarden buitgemaakt	* Cyber-aanvallen op banken, bijv. US 81 mio Central Bank of Bangladesh * Bij ons ook bekende WannaCry die 200.000 computers in 150 landen heeft geïnfecteerd

Neem de controle over uw data

Een pro-actieve benadering van preventie door gelaagde security oplossingen toe te passen is een slimme zet, maar houd rekening dat maar één ding veiligheid kan garanderen als hackers het lukt om binnen te komen: het hebben van een betrouwbaar back-up systeem. Met Veritas Backup Exec, kan bedrijfskritische data (zowel virtueel, fysiek en cloud workloads) geback-upped worden, weggehouden worden van ransomware en snel en eenvoudig teruggezet worden.

Air Gap Backups

Creëer een offline backup kopie van data en houd het buiten bereik van de productieomgeving

Multiple Copies

Bewaar kopieën van back-up images op verschillende lokaties om de kans tot toegang door de hacker te reduceren

Restrict Backup Credentials

Om phishing te minimaliseren, limiteer en monitor toegang tot backups continu

Shrink Your RPO

Vaker back-ups maken verkleint de RPO en reduceert potentieel dataverlies naar uren of zelfs minuten

Secure Your Backup Copies

Beveilig disk-gebaseerde back-ups tegen encryptie, wissen of modificeren door externe bronnen

Word weerbaar tegen ransomware met Veritas Backup Exec

https://www.bloomberg.com/news/articles/2021-05-08/u-s-fuel-sellers-scramble-for-alternatives-to-hacked-pipeline
https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html
https://searchsecurity.techtarget.com/feature/The-biggest-ransomware-attacks-this-year
https://threatpost.com/ransomware-victims-dont-pay-up/166989/
https://www.cybercoop.com/ransomware-extortion-demands-increasing-coveware/
https://www.theregister.com/2021/07/07/revil_tactics_and_multimillion_dollar/
https://www.theguardian.com/business/2021/jun/10/worlds-biggest-meat-producer-jbs-pays-11m-cybercrime-ransom
https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781
https://www.theguardian.com/technology/2021/jul/05/kaseya-ransomware-attack-explained-russia-hackers
https://www.forbes.com/sites/daveywinder/2021/07/03/70-million-demanded-as-revil-ransomware-attackers-claim-1-million-systems-hit/?sh=6b71897257c0
https://www.bbc.com/news/world-europe-57197688
https://www.zdnet.com/article/fbi-identifies-16-conti-ransomware-attacks-striking-us-healthcare-first-responders/
https://techcrunch.com/2020/11/02/maze-ransomware-group-shutting-down/
https://www.csoonline.com/article/3270584/what-does-a-ransomware-attack-cost-beware-the-hidden-expenses.html
https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/
https://www.bleepingcomputer.com/news/security/maze-ransomware-demands-6-million-ransom-from-southwire
https://www.wired.com/story/darkside-ransomware-colonial-pipeline-response/
https://www.npr.org/2021/06/09/1004684788/u-s-suffers-over-7-ransomware-attacks-an-hour-its-now-a-national-security-risk
https://www.technologyreview.com/2020/01/24/276082/lazarus-group-dragonex-chainalysis
https://www.zdnet.com/article/us-charges-two-more-members-of-the-lazarus-north-korean-hacking-group/
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

VERITAS
TechData A TD SYNNEX Company

1 (866) 837-4827
www.veritas.com