Tava uzņēmuma vairogs pret izspiedējprogramatūras uzbrukumu

Vadošais rezerves kopiju nodrošinātājs

> Risinājuma izvēli noteica Xopero fleksibilā pieeja iespējai modificēt risinājumu, lai to pielāgotu mūsu vajadzībām, un efektīvi ieviest testa versiju.

Paweł Kozieł, ICT Specialist
CEZ Skawina S.A. Power Plant

60+
valstīs

15gadi+
redzamība tirgū

10M+
aizsargātu iekārtu

200k+
gandarītu klientu

Drošība pirmajā vietā

GDPR

ISO 27001

SOC 2 Type II

High Performer
Spring-Summer 2022

5-star rating
backup

2022 Product
of the year

2019 Product/Service
of the year

Xopero galvenie partneri un klienti

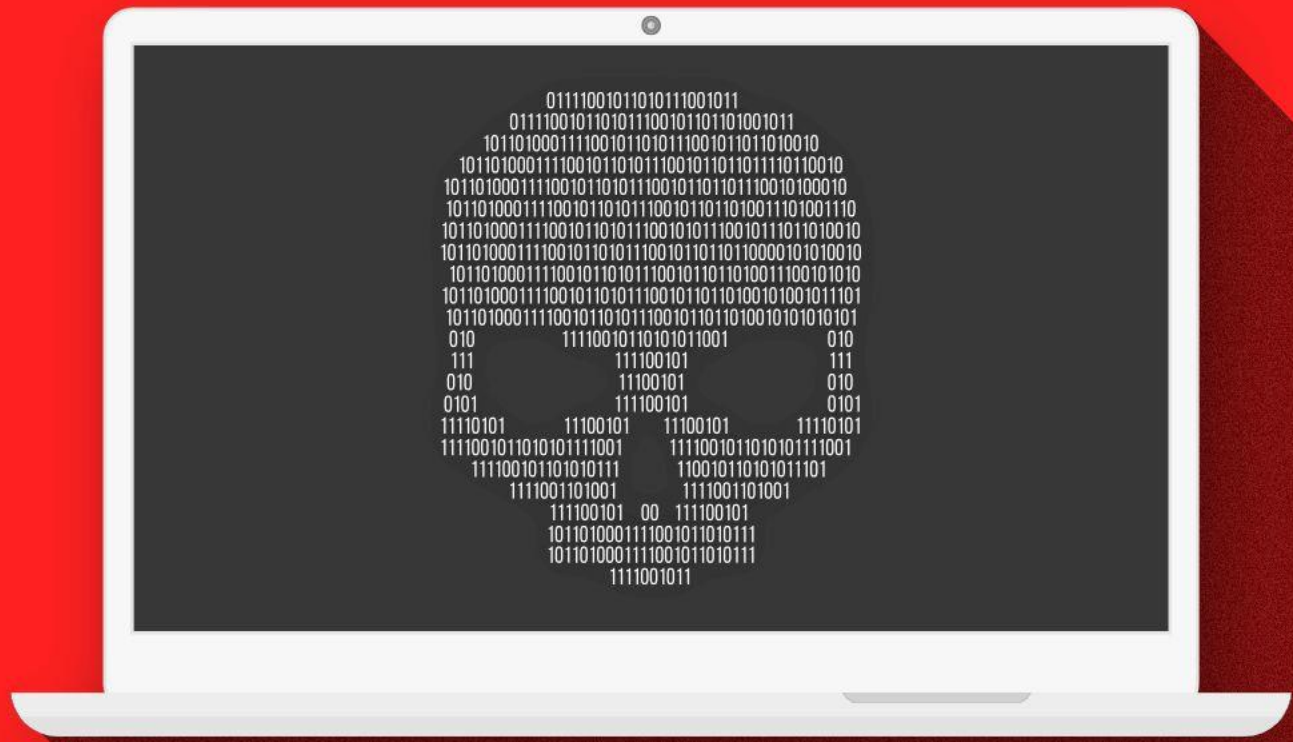
Galvenie partneri

Uzņēmumi

Publiskais sektors

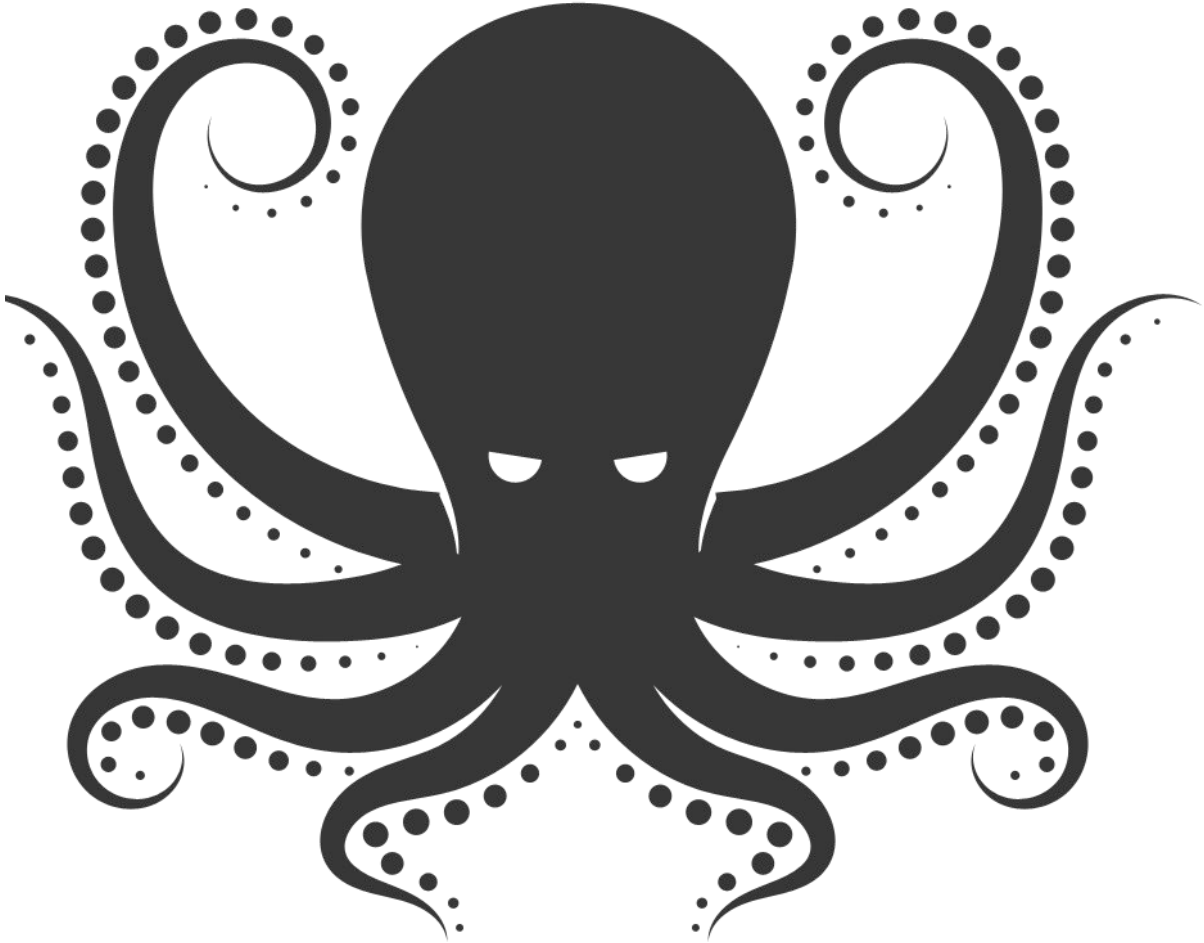
Rezerves kopijas infrastruktūrā: Kā izveidot to izspiedējvīrusu-drošu

ar Xopero ONE



Izspiedējvīruss/Ransomware

Kas tas ir ?



Izspiedējvīruss ir ļaunprātīga programmatūra, kas ierobežo piekļuvi inficētajai sistēmai vai datiem un pieprasa samaksāt izpirkuma maksu..

Izspiedējvīrussi

Attīstības hronoloģija

Izspiedējvīrussi

Uzbrukuma vektori

- Zināmas ievainojamības un nepilnības populāros pakalpojumos un operētājsistēmās,
- pikšķerēšanas e-pasta vēstules,
- autorizācijas datu noplūde un 2FA trūkums

Izspiedējvīrusi

Skaitļi runā skaļāk par tekstu

72% pasaules uzņēmumu 2023. gadā piedzīvoja izspiedējvīrusu uzbrukumus

30% uzņēmumu nav glābšanas plāna IT katastrofas gadījumā.

Tikai **4%** lietotāju veido rezerves kopijas katru dienu

Katrs darbinieks ziedo

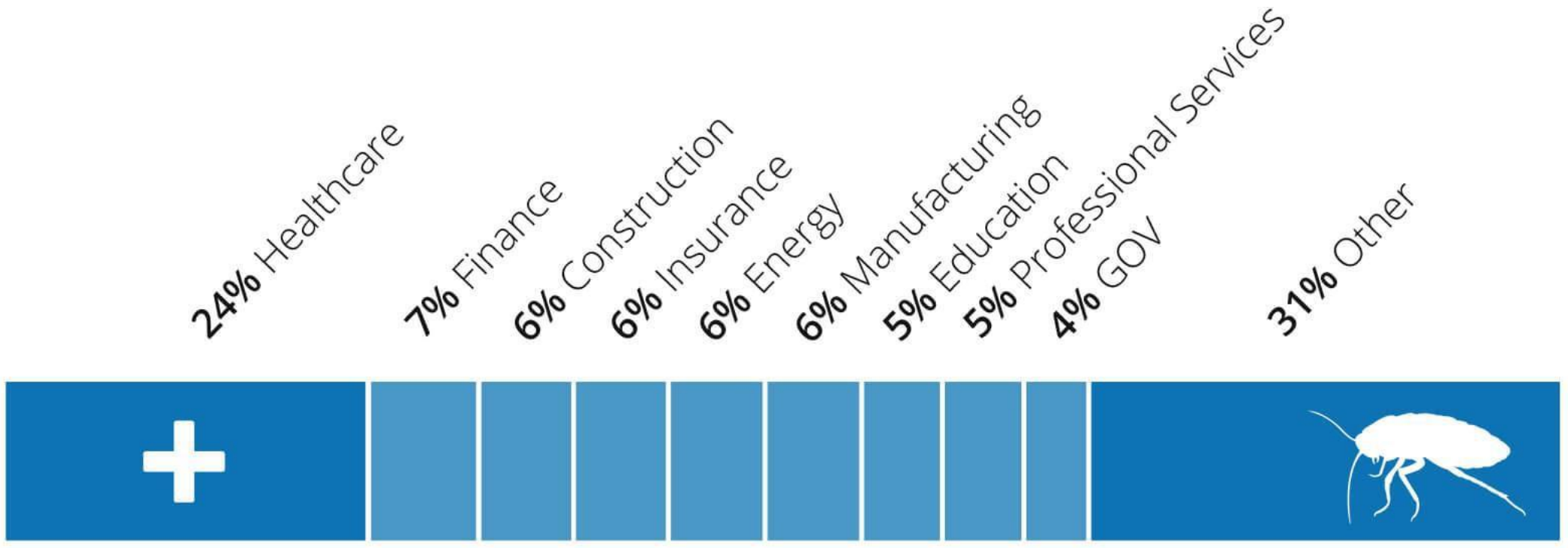
25% no savas darba dienas, lai atjaunotu zaudētos datus.

94% izspiedējvīrusu ietver sevī mēģinājumu šifrēt dublējuma repozitoriju.

$ 1.85 miljoni ir

vidējā uzņēmumu izpirkuma maksa 2023. gadā

Kam uzbrūk izspiedējvīrusi (pēc nozares)



Avots: Symantec

Katrs € 1 = € 4

Rezerves kopēšanas risinājumam iztērētie līdzekļi stratēģija

Reakcijas un atjaunošanas izmaksu ietaupījums

10 padomi lai aizsargātu sevi pret izspiedējvīrusiem

Nemaksājiet izpirkuma maksu. Jums nav garantijas, ka atgūsiet savus datus.

Veiciet dublēšanu katru dienu. Iestatiet automātiskās dublēšanas uzdevumu.

Izveidojiet diska tēlu. Lai ātrāk atjaunotu datoru, varat virtualizēt fizisku ierīci.

Pārliecinieties, ka izmantojat drošu un uzticamu pretvīrusu programmu.

Regulāri atjauniniet operētājsistēmu. Hakeri iecienījuši atvērtas sistēmas ievainojamības.

Esiet modri. Analizējiet e-pasta ziņojumus. Neklikšķiniet uz aizdomīgām saitēm un pielikumiem.

Ikdienā izmantojiet lietotāja kontu (nevis administratora kontu).

Rūpīgi piešķiriet atļaujas uzņēmuma tīkla resursiem.

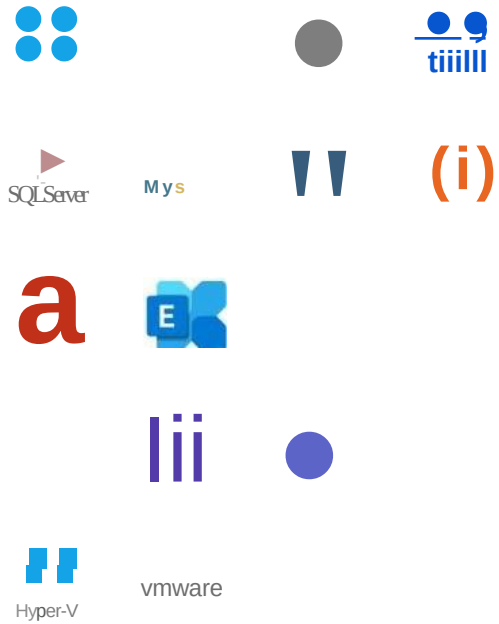
Izslēgt attālo darbvirsmu. Neaizsargāts RDP protokols ir iecienīts hakeru “aizmugurējais vārtiņš”.

Ja ir aizdomas par izspiedējvīrusa uzbrukumu, nekavējoties izslēdziet datoru no tīkla.

Esat gatavi ar

Xopero ONE

Xopero ONE

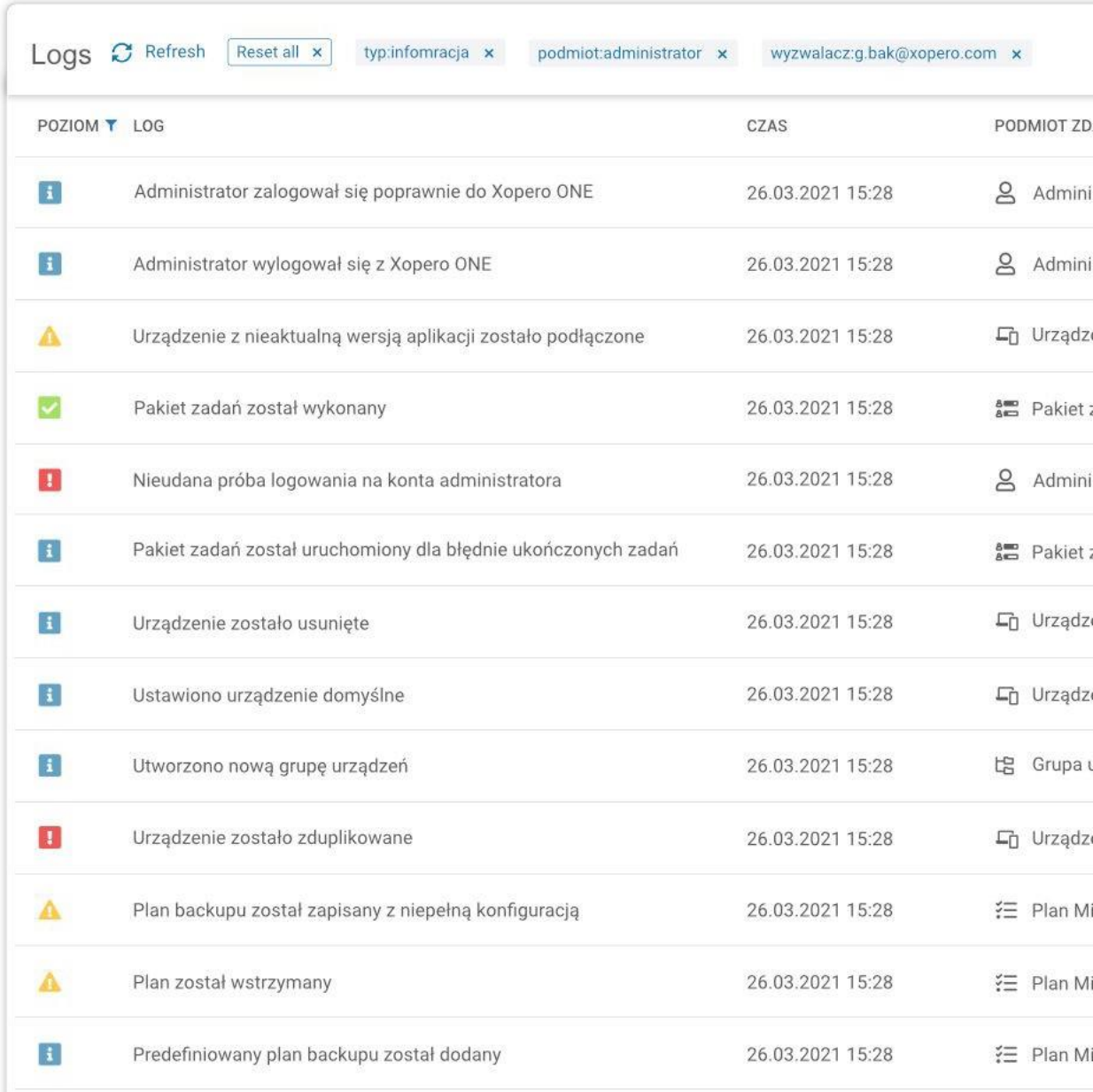


Dedicated PortalMSP

Tehnoloģiju ekosistēma bez funkcijām

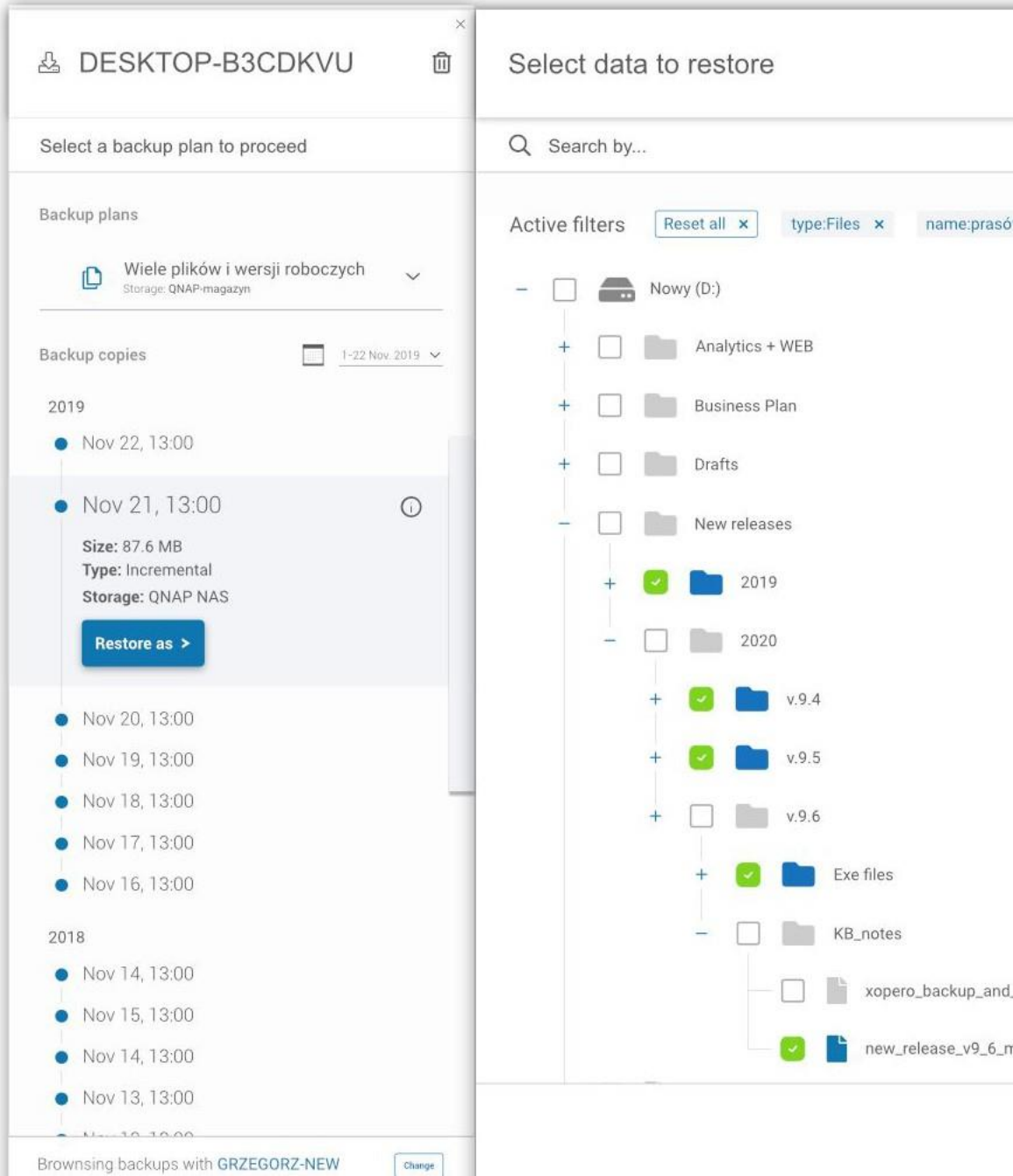
Izspiedējvīrusu aizsardzība

- Neizpildāmo failu dublējumkopijas
- Uzglabāšana Nemainīga krātuve (WORM)
- Vairāki dublēšanas galamērķi
- Tūlītēja rezerves kopiju verifikācija
- Uzglabāšanas autentificēšana - dati, kas tiek glabāti ārpus dublēšanas aģenta.
- Tūlītējas & pilnas atjaunošanas
- Atjaunošana kā Serviss



Elastīga atjaunošana & datu katastrofu atjaunošana

- Any2Any atjaunošana
- File/Image atjaunošana
- Attālinātā atjaunošana
- BMR – Bare metal recovery
- Elastīgā diska atjaunošana
- Granulārā atjaunošana



q&a

paldies