



**Tava uzņēmuma vairogs
pret
izspiedējprogramatūras
uzbrukumu**

Vadošais rezerves kopiju nodrošinātājs



60+

valstis



15gadi+

redzamība
tirgū



10M+

aizsargātu
iekārtu



200k+

gandarītu
klientu

”

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

Paweł Koziel, ICT Specialist

CEZ Skawina S.A. Power Plant

Drošība pirmajā vietā



GDPR

ISO

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



GitHub



Logicom

QNAP



SUBWAY



AVIS



Klar



Uzņēmumi



FORMASTER GROUP



NORTH FOOD



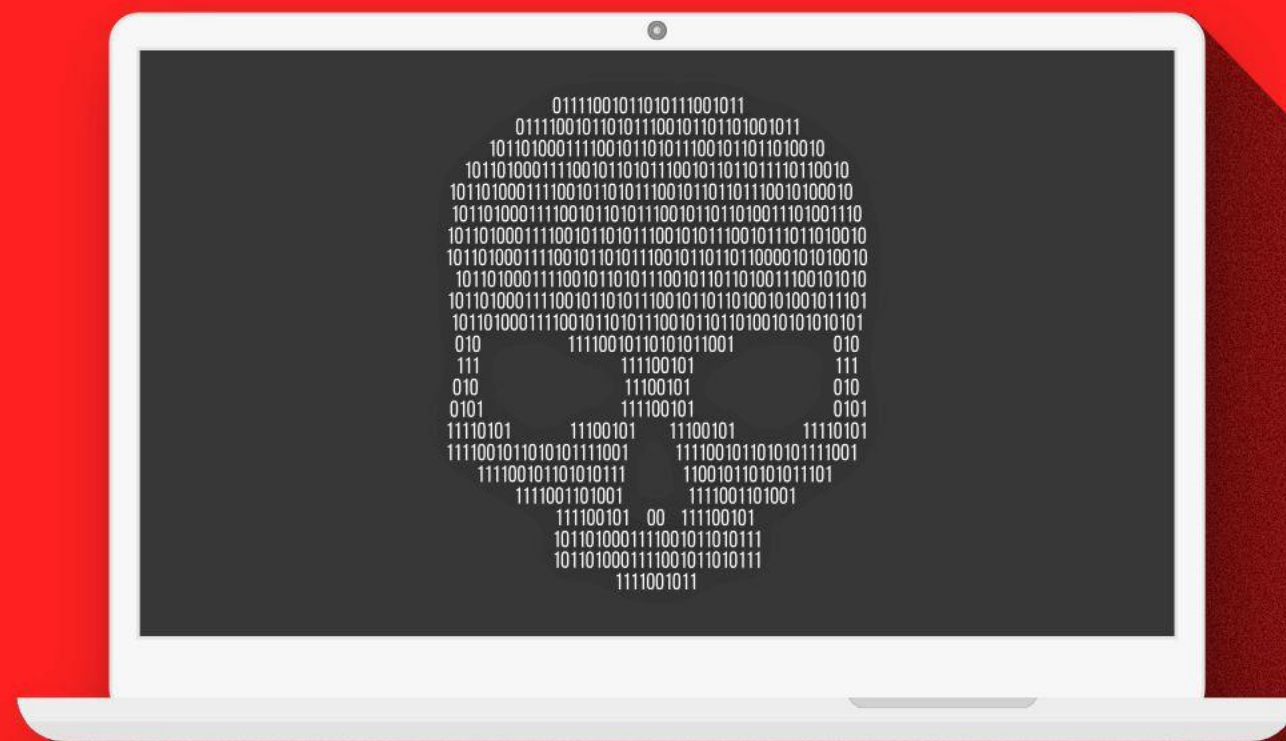
Publiskais sektors

GLADSTONE INSTITUTES



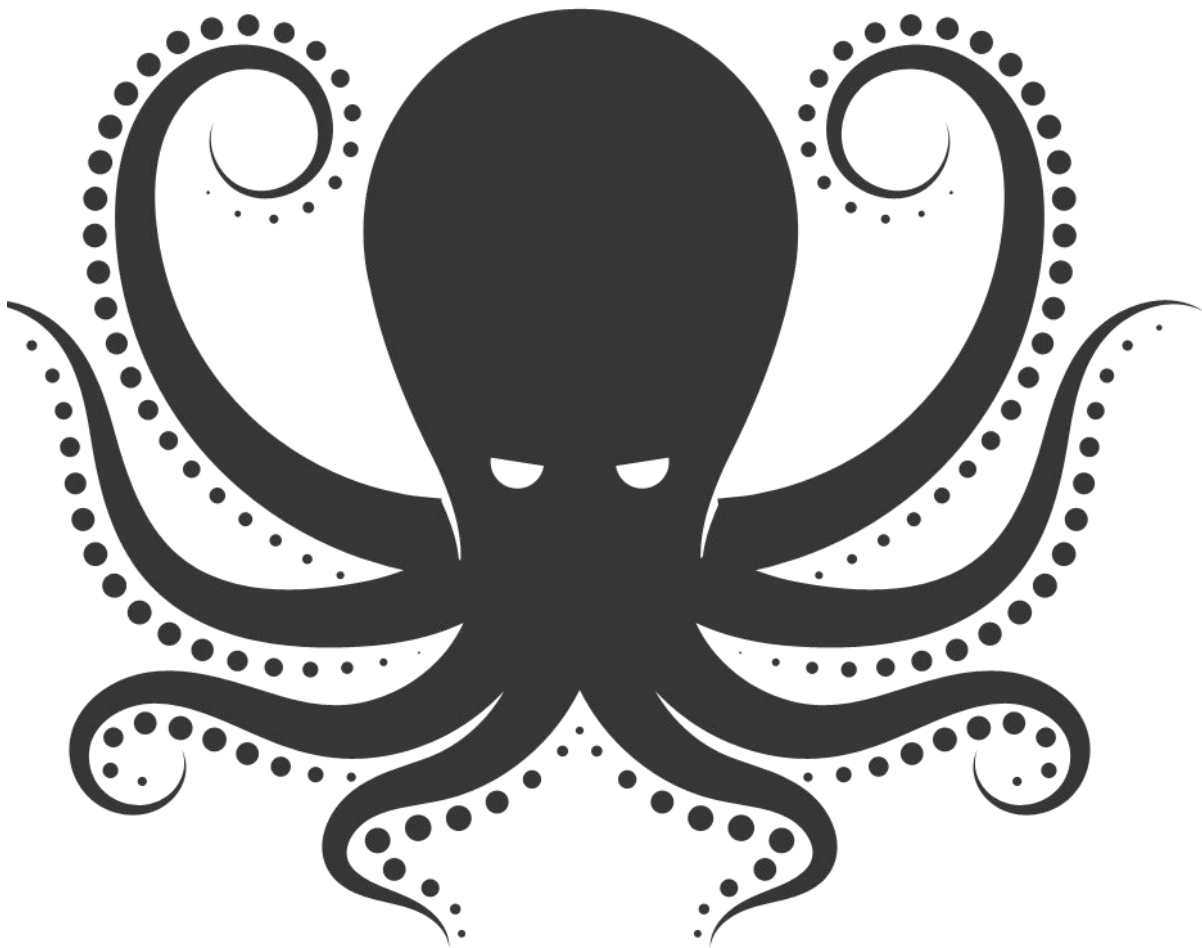
Rezerves kopijas infrastruktūrā: Kā izveidot to izspiedējvīrusu- drošu

ar Xopero ONE



Izspiedējvīruss/Ransomware


Kas tas ir ?



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

Izspiedējvīrusi
Attīstības hronoloģija

1989
 AIDS Trojas zirgs - pirmā izspiedējvīrusa programmatūra

1992
 Ideja par anonīmu naudas sistēmu

1996
 Publiskās atslēgas kriptogrāfija datu zādzībās

2005
 Izspiedējprogrammatūra izmanto spēcīgas RSA atslēgas.

2013
 CryptoLocker

Izspiedējvīrusi

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.



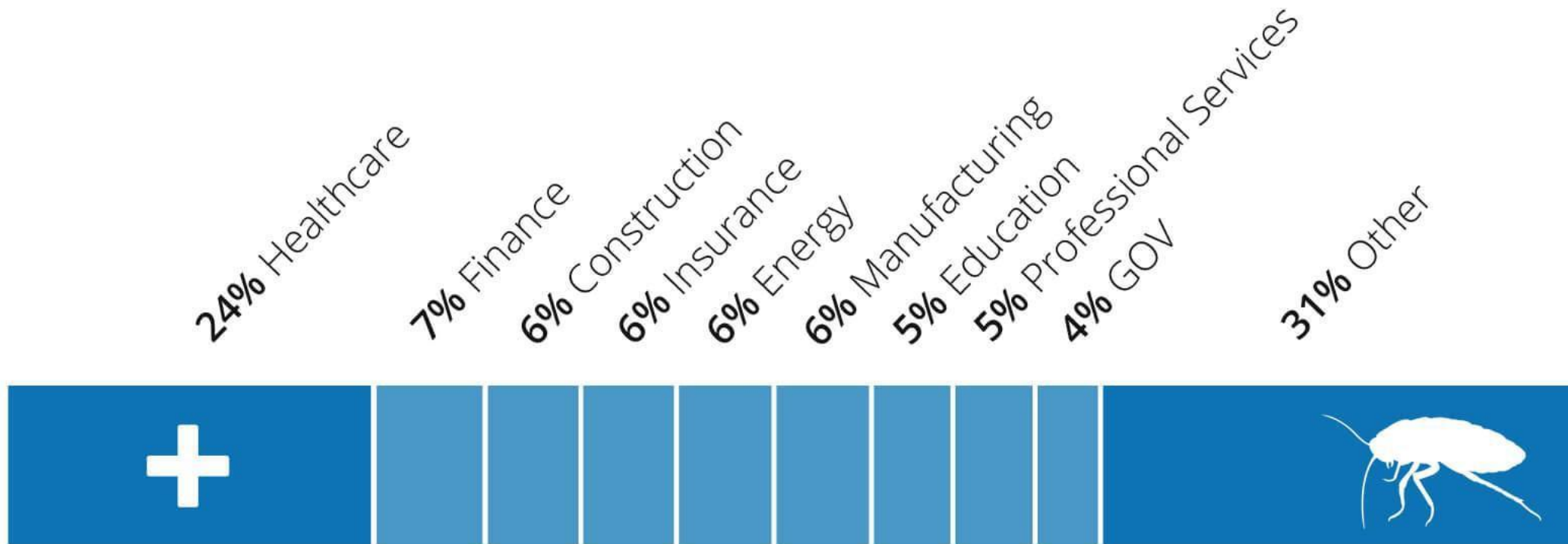
94% izspiedējvīrusu ietver
sevi mēģinājumu šifrēt
dublējuma repositoiju.



\$ 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.



Pārlicinieties, 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 darbvirsu. Neaizsargāts RDP protokols ir iecienīts hakeru "aizmugurējais vārtiņš".



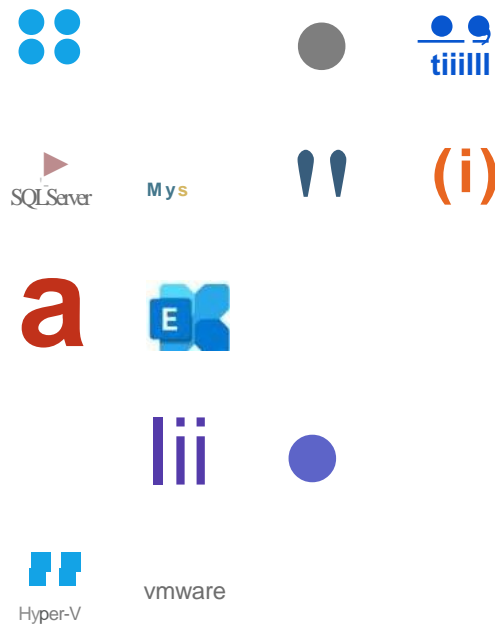
Ja ir aizdomas par izspiedējvīrusa uzbrukumu, nekavējoties izslēdziet datoru no tīkla.



Esat gatavi ar
Xopero ONE



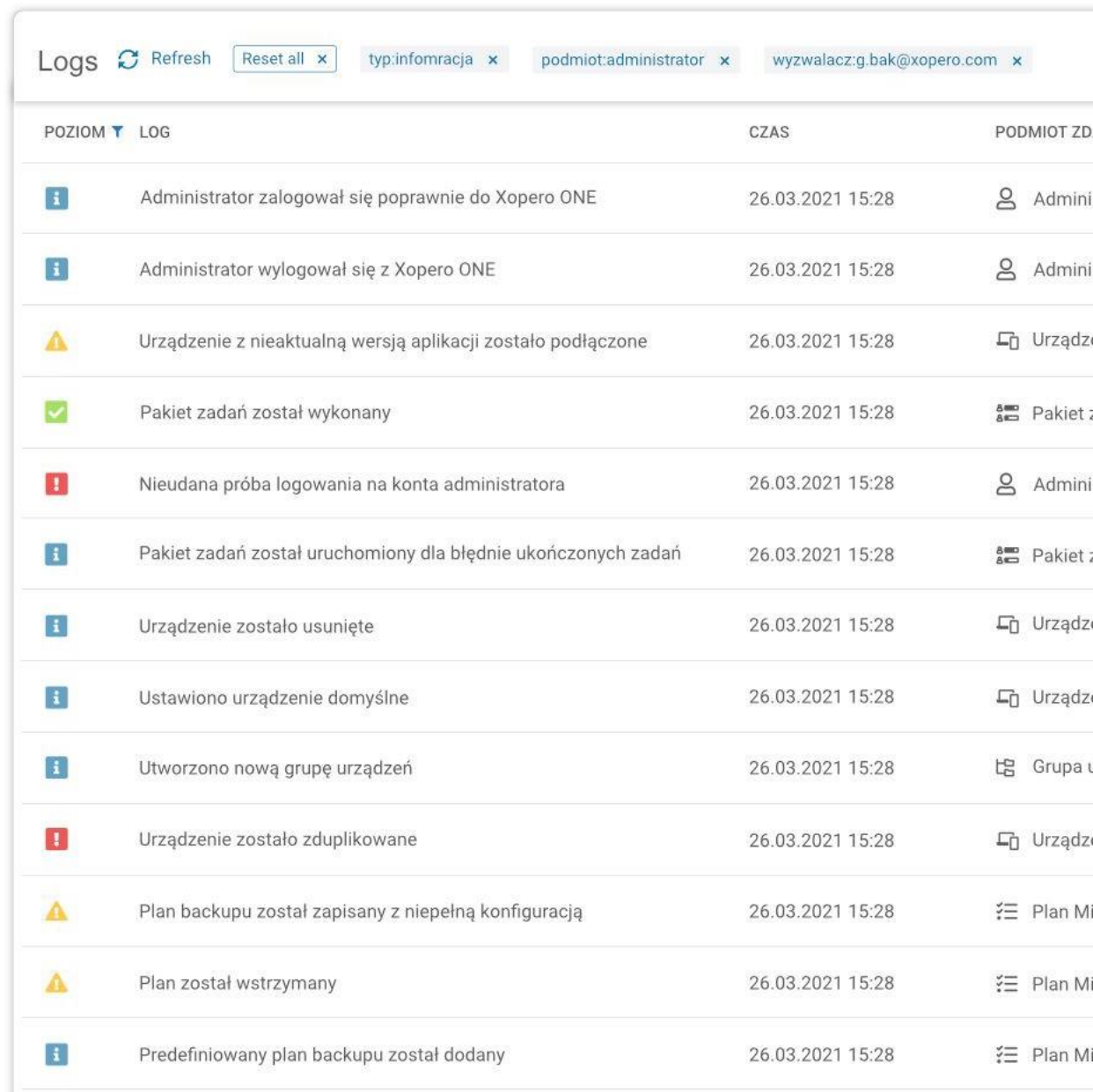
Xopero ONE



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



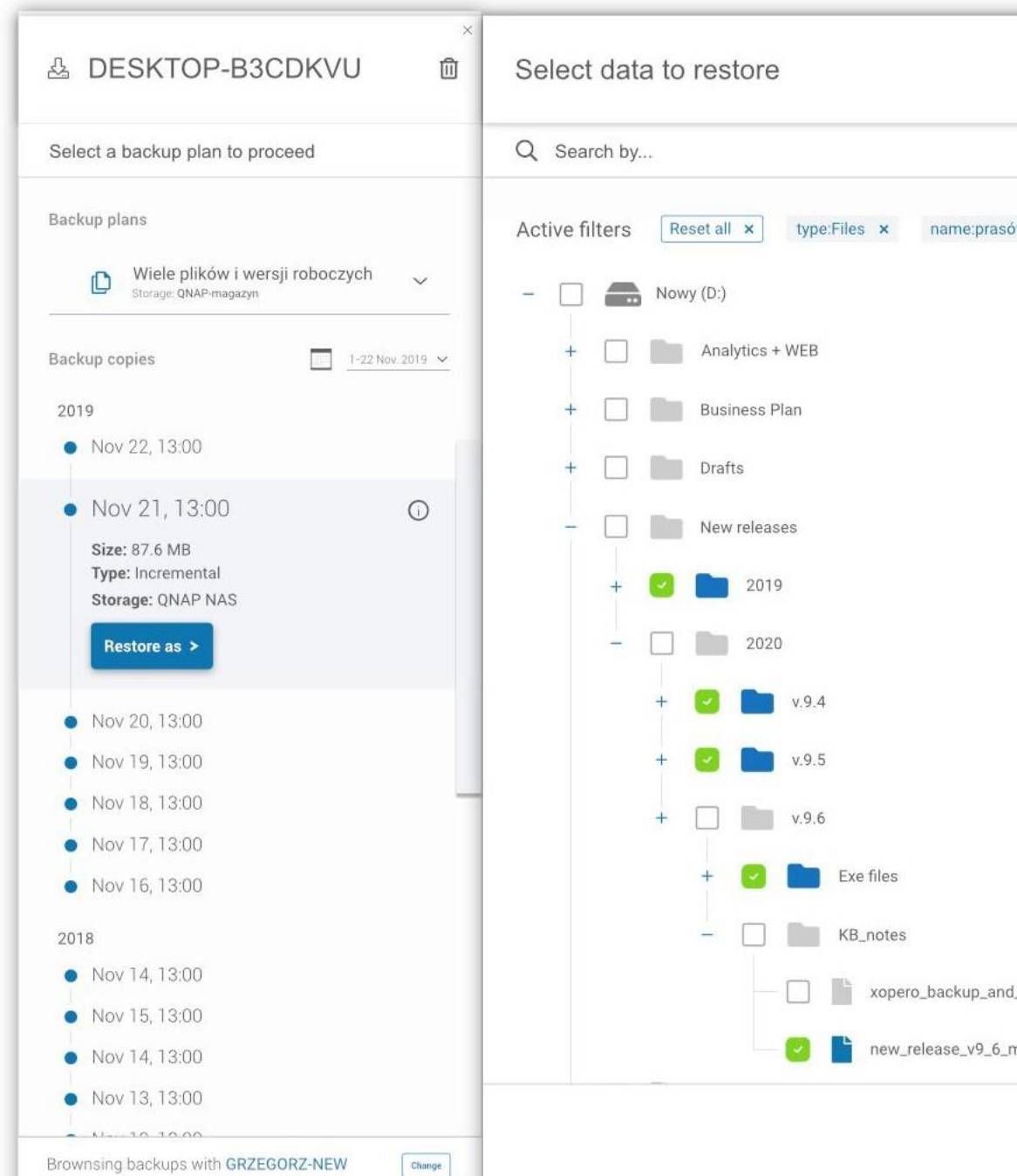
The screenshot shows a log interface with the following elements:

- Buttons: Logs, Refresh, Reset all
- Filters: typ:informacja, podmiot:administrator, wyzwalacz:g.bak@xopero.com
- Table columns: POZIOM LOG, CZAS, PODMIOT ZD
- Log entries with icons (info, warning, error, success) and descriptions.

POZIOM LOG	CZAS	PODMIOT ZD
Administrator zalogował się poprawnie do Xopero ONE	26.03.2021 15:28	Admini
Administrator wylogował się z Xopero ONE	26.03.2021 15:28	Admini
Urządzenie z nieaktualną wersją aplikacji zostało podłączone	26.03.2021 15:28	Urządze
Pakiet zadań został wykonany	26.03.2021 15:28	Pakiet z
Nieudana próba logowania na konta administratora	26.03.2021 15:28	Admini
Pakiet zadań został uruchomiony dla błędnie ukończonych zadań	26.03.2021 15:28	Pakiet z
Urządzenie zostało usunięte	26.03.2021 15:28	Urządze
Ustawiono urządzenie domyślne	26.03.2021 15:28	Urządze
Utworzono nową grupę urządzeń	26.03.2021 15:28	Grupa u
Urządzenie zostało zduplikowane	26.03.2021 15:28	Urządze
Plan backupu został zapisany z niepełną konfiguracją	26.03.2021 15:28	Plan M
Plan został wstrzymany	26.03.2021 15:28	Plan M
Predefiniowany plan backupu został dodany	26.03.2021 15:28	Plan M

Elastīga atjaunošana & datu katastrofu atjaunošana

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



q&a

paldies