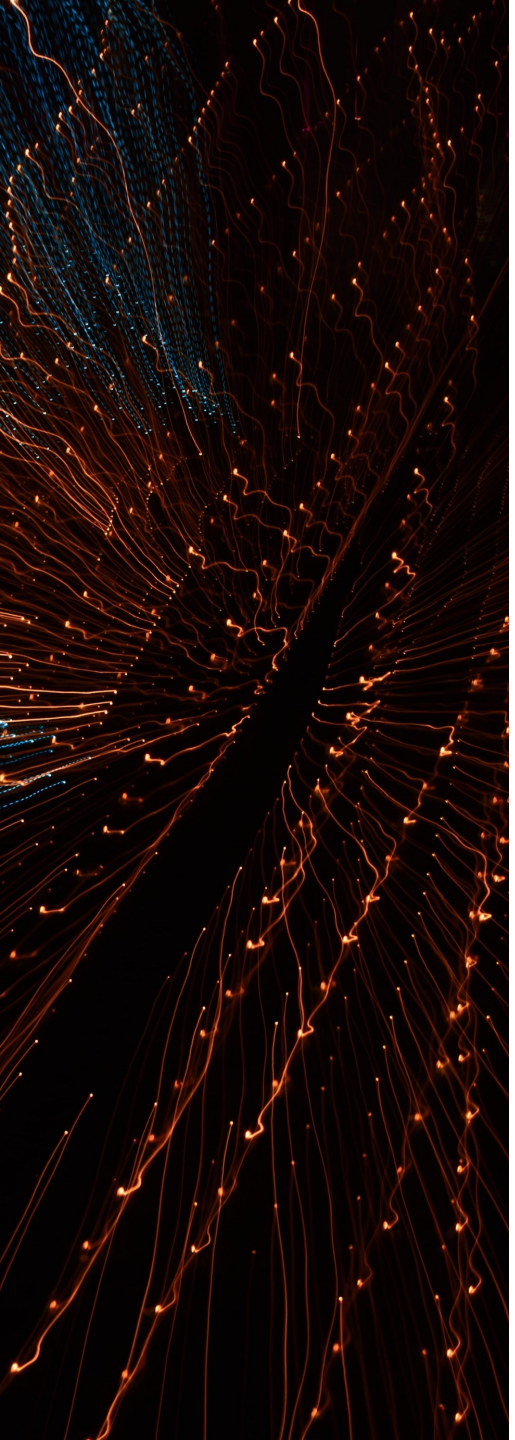
CIĄGŁOŚĆ OPERACYJNA SIECI I INFRASTRUKTURY BEZPIECZEŃSTWA

BACKBOX

Wojciech Siwiński

NetFormers

NETFORMERS



96% organizacji twierdzi, że skalowanie działalności jest niemożliwe bez automatyzacji [1]

93% specjalistów jest niezadowolonych z obecnego podejścia ich organizacji do automatyzacji [1]

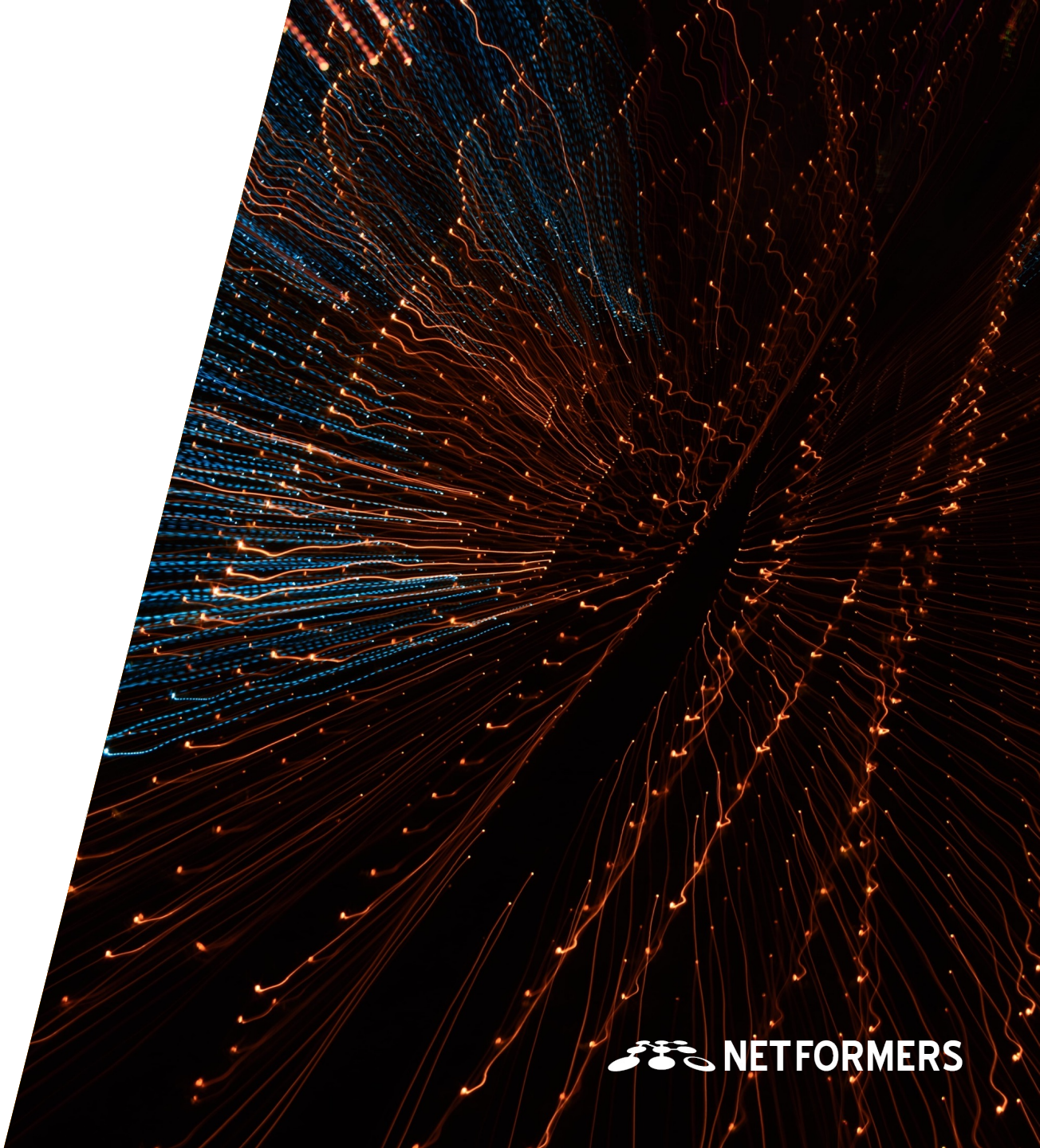
[1] BackBox survey 2023

NETFORMERS

CIĄGŁOŚĆ OPERACYJNA

01 **Zapobieganie przestojom**

02 **Przywracanie operacyjności**



NIS2

Art. 21, Ust 2.
Środki, o których mowa w ust. 1, opierają się na podejściu uwzględniającym wszystkie zagrożenia, które ma na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują
co najmniej następujące elementy:

(…)

ciągłość biznesowa, taka jak zarządzanie kopiami zapasowymi
i odtwarzaniem po awarii oraz zarządzanie kryzysowe;

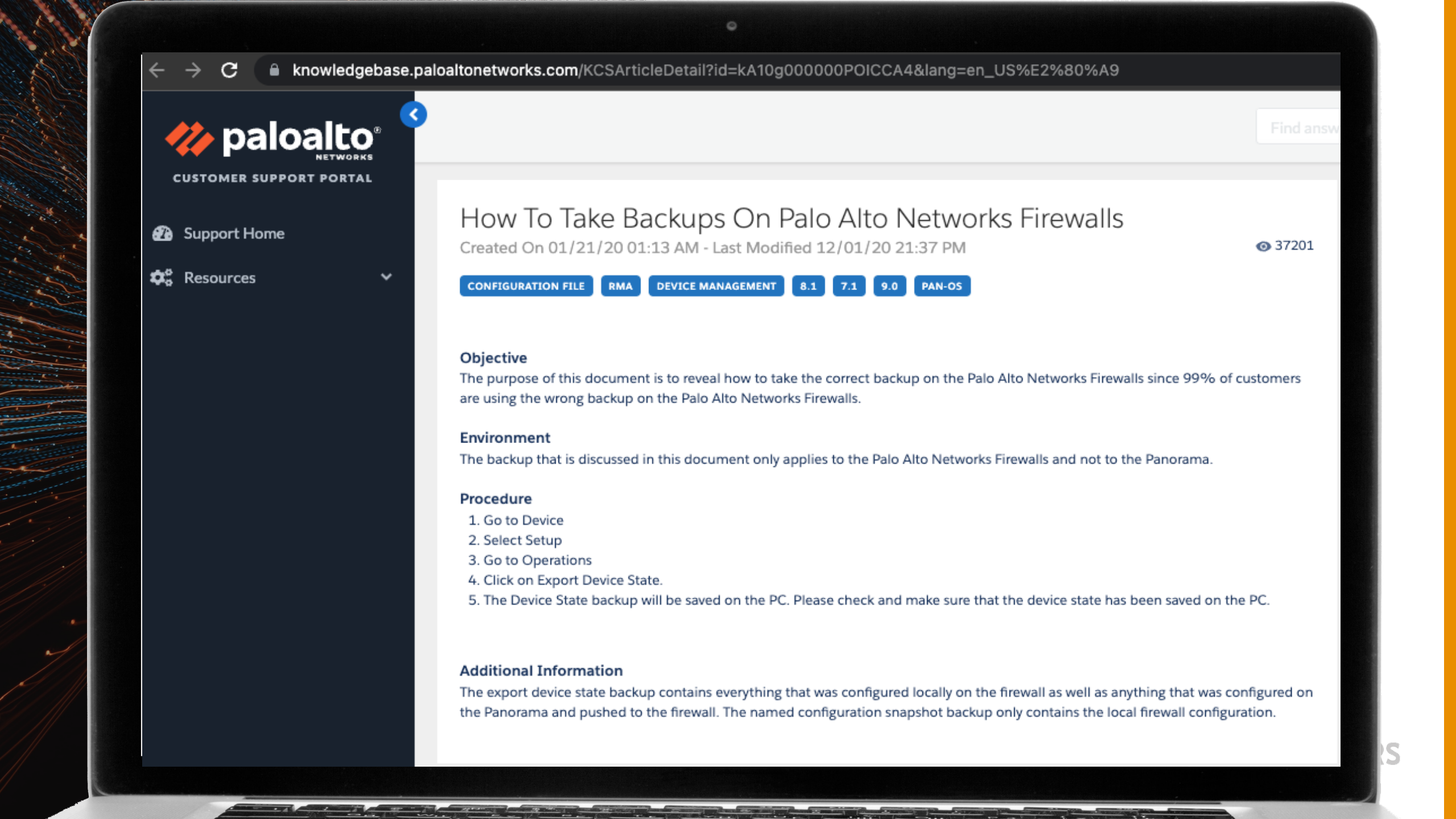
(…)

NETFORMERS

Czy robisz backup'y ?

Konfiguracji urządzeń
Sieciowych i Bezpieczeństwa?

NETFORMERS


knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000POICCA4&lang=en_US%E2%80%A9
paloalto NETWORKS
CUSTOMER SUPPORT PORTAL
Support Home
Resources
How To Take Backups On Palo Alto Networks Firewalls
Created On 01/21/20 01:13 AM - Last Modified 12/01/20 21:37 PM
37201
CONFIGURATION FILE
RMA
DEVICE MANAGEMENT
8.1
7.1
9.0
PAN-OS
Objective
The purpose of this document is to reveal how to take the correct backup on the Palo Alto Networks Firewalls since 99% of customers are using the wrong backup on the Palo Alto Networks Firewalls.
Environment
The backup that is discussed in this document only applies to the Palo Alto Networks Firewalls and not to the Panorama.
Procedure
1. Go to Device
2. Select Setup
3. Go to Operations
4. Click on Export Device State.
5. The Device State backup will be saved on the PC. Please check and make sure that the device state has been saved on the PC.
Additional Information
The export device state backup contains everything that was configured locally on the firewall as well as anything that was configured on the Panorama and pushed to the firewall. The named configuration snapshot backup only contains the local firewall configuration.

Backup

3

Kopie

2

Różne systemy

1

Lokalizacja offsite

w tym cloud

NETFORMERS

Twoje Backup'y

Czy na pewno możesz im ufać?

- Czy posiadam aktualną kopię konfiguracji?
- Czy wszystkie urządzenia (również VA) są uwzględnione?
- Czy moje dane są kompletne i wystarczające?
- Czy weryfikuję wykonane backupy?
- Gdzie się znajdują?
- Czy są zabezpieczone przed ingerencją?
- Kto i w jakiej sytuacji ma do nich dostęp?

Czy robisz backup'y konfiguracji urządzeń Sieciowych i Bezpieczeństwa?

... A jaka jest Twoja polityka odtwarzania?

NETFORMERS

Przywracalność

Czy mam na czym się odtworzyć?

Czy mam z czego się odtworzyć?

Czy mam wiedzę i zasoby aby połączyć powyższe elementy?

… jaki jest mój **oczekiwany czas** przywrócenia?

[1] BackBox survey 2023

Tylko 20% firm jest przekonanych o możliwości przywrócenia elementów infrastruktury w czasie pojedynczych minut[1]

NETFORMERS

Standaryzacja

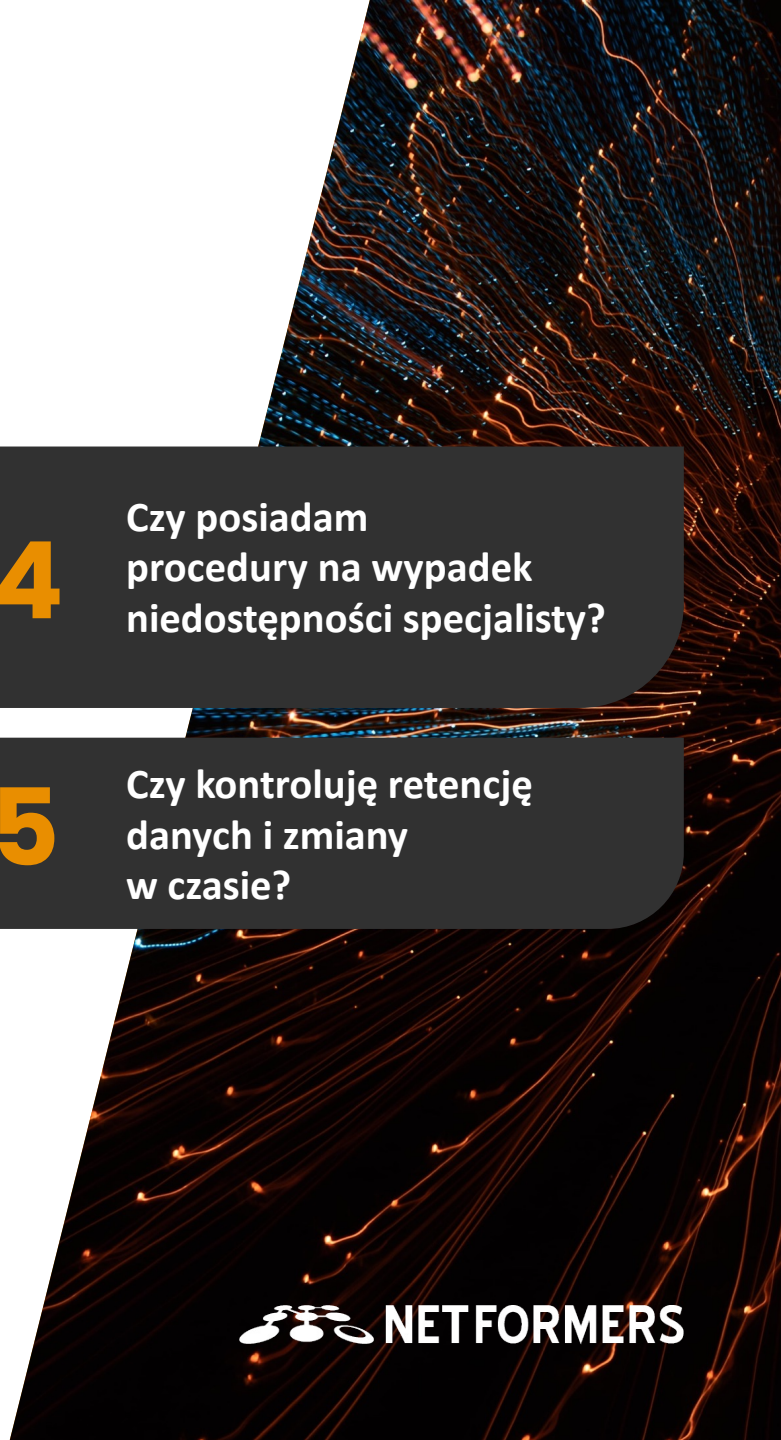
01 Czy utrzymuję jednolity standard tworzenia i przechowywania kopii zapasowych dla całej infrastruktury sieciowej komponentów bezpieczeństwa?

02 Czy mam spójne i jednolite procedury przywracania i odpowiednią dokumentację?

03 Czy dokumentacja jest dostępna i odpowiednio skatalogowana?

04 Czy posiadam procedury na wypadek niedostępności specjalisty?

05 Czy kontroluję retencję danych i zmiany w czasie?



NETFORMERS

Ciągłość operacyjna

Ciągłość operacyjna to nie tylko backup i procedury odtwarzania!

Jest to głównie codzienne utrzymywanie systemów!

NETFORMERS

Poprawki i aktualizacje OS

92% **twierdzi, że potrzeba większej ilości aktualizacji,** niż są w stanie wykonać[1]

53% **aktualizuje swoje urządzenia sieciowe** i bezpieczeństwa co kwartał lub rzadziej[1]

56% **firm przyznało, że gdy ich firma doświadczyła naruszenia w obszarze cyberbezpieczeństwa,** było to spowodowane wykorzystaniem znanej luki w zabezpieczeniach[1]

51% organizacji IT przyznaje że ma problem z **niedoborem zasobów ludzkich w zakresie cyberbezpieczeństwa** [1]

Narzędzia do automatyzacji sieci zwiększają elastyczność i wydajność, obniżają koszty i redukują liczbę błędów. Automatyzacja sieci w przedsiębiorstwach pozostaje w tyle za automatyzacją serwerów *[...]. Ograniczanie automatyzacji sieci tworzy możliwe do uniknięcia wąskie gardła w udostępnianiu i rozwiązywaniu incydentów, jednocześnie zwiększając prawdopodobieństwo wystąpienia błędów ludzkich.*

| *Gartner, June 2022*

Zalecamy automatyzację czynności, które przynoszą szybkie korzyści (quick win), takich jak diagnostyka, tworzenie kopii zapasowych i archiwizacja.

NETFORMERS

[1]ISSA [2]Gartner

Jakie korzyści płyną ze skutecznej Automatyzacji urządzeń sieciowych i bezpieczeństwa?

NETFORMERS

- **Minimalizacja czasu przestoju** i MTTR poprzez automatyzację procedur przywracania
- **Skrócenie** i optymalizacja okien serwisowych
- **Ograniczanie błędów** ludzkich w codziennych działaniach
- **Zapewnienie zgodności konfiguracji** z wewnętrznymi i zewnętrznymi regulacjami (skrócenie czasu i kosztu audytu)
- Zapewnienie Tobie i Twojemu zespołowi **aktualnych informacji i natychmiastowej wiedzy operacyjnej**
- Odciążenie zespołu z **powtarzalnych, rutynowych zadań**
- **Automatyzacja funkcjonalności** urządzeń zależnych od ręcznych czynności

Higiena automatyzacji

- Efektywność, łatwość tworzenia i personalizacji
- Bezpieczeństwo, kontrola, audytowalność i rozliczalność zarówno podczas tworzenia automatyzacji, jak i jej wykorzystywania
- Koszty i wysiłek związany z utrzymaniem
- Skalowalność
- Krzywa uczenia się użytkowników
- Wsparcie !!!

NETFORMERS

01 **Czy stać mnie na tworzenie**, utrzymywanie i rozwój własnych rozwiązań w obszarze Automatyzacji?

02 **Czy jestem świadomy całkowitego kosztu posiadania (TCO),** w tym wszystkich ukrytych kosztów i ryzyka związanego z samodzielnie opracowanymi rozwiązaniami?

NETFORMERS

NIS2

Art. 21, Ust 2.

Środki, o których mowa w ust. 1, opierają się na podejściu uwzględniającym wszystkie zagrożenia, które ma na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: (wybrane)

- Ciągłość biznesowa, taka jak zarządzanie kopiami zapasowymi i odtwarzaniem po awarii oraz zarządzanie kryzysowe
- Bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące relacji między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;
- Bezpieczeństwo w pozyskiwaniu, rozwijaniu i utrzymywaniu sieci i systemów informatycznych, w tym zarządzanie i obsługa podatności;
- Bezpieczeństwo zasobów ludzkich, zasady kontroli dostępu i zarządzanie zasobami;
- Polityki i procedury dotyczące korzystania z kryptografii i w stosownych przypadkach, szyfrowania;

NETFORMERS

BACKBOX

Dlaczego warto wybrać BackBox do zaufanej automatyzacji sieci i urządzeń bezpieczeństwa?

BackBox to specjalnie zaprojektowane rozwiązanie do automatyzacji z obsługą blisko 200 producentów i biblioteką automatyzacji (Automation Library™) **zawierającą ponad 3000 gotowych do użycia automatyzacji.**

ASTORS AMERICAN SECURITY TODAY 2022 PLATINUM AWARD WINNER HOMELAND SECURITY AWARDS

TOP INFOSEC INNOVATOR WINNER CYBER DEFENSE MAGAZINE 2023

- BEST IN CLASS BACKUP & RESTORE
- SOPHISTICATED PRE-BUILT OS UPDATE AUTOMATIONS
- CIS BENCHMARK™ AUTOMATIONS PRE-BUILT FOR ALL TOP VENDORS
- DYNAMIC INVENTORY ENRICHES CMBD, REPORTING, OR ANY ITSM VIA API
- CLOSED-LOOP VULNERABILITY MITIGATION
- AUTO-DISCOVERY AND TRACKING OF MOVES, ADDS, & CHANGES
- CONFIGURATION DRIFT REPORTING & AUTO-REMEDIATION
- TASK AUTOMATION

NETFORMERS

Zaproszenie

Dedykowane warsztaty z technologii

BackBox

w siedzibie NetFormers
Mińska 75, Warszawa

w dniu 28.05.2024 r.

Dziękuję bardzo !

Zapraszamy do współpracy