Czym jest NIS2 i na które sektory ma wpływ?

Dyrektywa UE w sprawie bezpieczeństwa sieci i systemów informatycznych (NIS) została pierwotnie wprowadzona w 2016 r. jako pierwsze ogólnounijne przepisy dotyczące cyberbezpieczeństwa. Ustanowiła ona obowiązki w zakresie cyberbezpieczeństwa dla operatorów "usług kluczowych" w sektorach krytycznych (takich jak energetyka, transport, zdrowie i finanse) oraz dla dostawców usług cyfrowych (internetowych platform handlowych, wyszukiwarek i usług w chmurze).

Uznając, że krajobraz cyberzagrożeń znacznie się zmienił od czasu przyjęcia pierwszej dyrektywy NIS, w grudniu 2020 r. Komisja Europejska zaproponowała zmienioną dyrektywę NIS (NIS2).

Nowa dyrektywa rozszerzyła liczbę objętych nią sektorów

- Administracje publiczną,
- Dostawców usług zarządzania ściekami i odpadami,
- Publiczne sieci łączności elektronicznej lub dostawcy usług,
- Producenci krytycznych produktów, takich jak farmaceutyki, wyroby medyczne, chemikalia,
- Producenci żywności,
- Usługi cyfrowe, takie jak platformy społecznościowe i centra danych,
- Dostawców infrastruktury kosmicznej,
- Usługi pocztowe i kurierskie.

NIS2 weszła w życie 16 stycznia 2023 r., a państwa członkowskie UE mają czas do 17 października 2024 r. na wprowadzenie dyrektywy do prawa krajowego.

Jakie są kluczowe wymagania NIS2?

NIS2 ustanawia cztery nadrzędne wymagania dla organizacji:

1. Podjęcie działań w celu zminimalizowania ryzyka cybernetycznego, w tym w łańcuchu dostaw ICT.
2. Wdrożenie procesów zgłaszania incydentów cyberbezpieczeństwa do ENISA (European Union Agency for Cybersecurity):
   a) W ciągu 24 godzin -> dostarczyć ENISA "raport wczesnego ostrzegania"
   b) W ciągu 72 godzin -> dostarczyć ENISA pełniejsze "powiadomienie o incydencie"
   c) W ciągu 1 miesiąca -> dostarczyć ENISA "raport końcowy" ze szczegółowym opisem incydentu, w tym jego powagi, wpływu i wdrożonych środków łagodzących.
3. Ustanowienie systemu odpowiedzialności korporacyjnej, który nadzoruje, zatwierdza i szkoli pracowników w zakresie środków cyberbezpieczeństwa

Jak Storware może pomóc w spełnieniu normy NIS2?

Storware Backup and Recovery to Polskie, łatwe w zarządzaniu i automatyzacji oprogramowanie do backupu i przywracania danych dla środowisk wirtualnych, kontenerowych oraz pamięci masowych.

1. **Storware Backup and Recovery** rozwiązanie to umożliwia składowanie kopii zapasowych w wielu lokalizacjach, takich jak: lokalny system plików lub NFS/CIFS, obiektowa pamięć masowa lub inne systemy kopii zapasowych klasy enterprise, jak m.in. Dell, IBM czy Micro Focus.

2. **Storware Backup and Recovery umożliwia tworzenie kopii zapasowych danych biznesowych pakietu Microsoft 365:** Exchange Online, OneDrive for Business, Microsoft Teams oraz SharePoint Online. Umożliwia także ochronę danych na urządzeniach końcowych, takich jak komputery stacjonarne i laptopy, a dzięki funkcji Continuous Data Protection (CDP) czy natywnemu mechanizmowi redukcji danych (deduplikacja i kompresja) gwarantuje solidną ochronę danych dla całej organizacji.

Zaufali nam:

Bank Pekao

IB PAN

EUROPA UBEZPIECZENIA

Politechnika Warszawska

USP Zdrowie

CISCO

Piotr Luc
Product Manager – CONNECT DISTRIBUTION
e-mail: p.luc@connectdistribution.pl
tel.: 22 400 1234
tel. kom.: 787 003 909