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

BlackBerry | Cybersecurity

Jak BlackBerry może pomóc w spełnieniu normy NIS2?

BlackBerry pomaga firmom, agencjom rządowym i instytucjom o kluczowym znaczeniu dla bezpieczeństwa każdej wielkości zabezpieczyć swoje organizacje i reagować w sytuacjach kryzysowych. Możemy pomóc Twojej organizacji w następujący sposób:

1. Zapobiegaj cyberatakom, zanim do nich dojdzie, dzięki CylanceENDPOINT (nextgenAV, EDR), samoobronnemu rozwiązaniu opartemu na AI od BlackBerry do ochrony punktów końcowych, które wykrywa zagrożenia, zanim spowodują szkody, minimalizując zakłócenia w działalności i koszty poniesione w wyniku ataku ransomware.

Zaufali nam:

Gartner Peer Insights Customers' Choice 2023

Linnovate Partners

County of Fairfax 1742 Virginia

reece group

2. Reaguj na incydenty i wdrażaj plany ciągłości działania dzięki (CEM), rozwiązaniu do zarządzania krytycznymi zdarzeniami (critical event management), które łączy bezpieczny system powiadomień alarmowych z narzędziami do reagowania na incydenty - dzięki czemu Twoja organizacja może szybko wdrożyć zespoły reagowania i umożliwić im lepsze przygotowanie, reagowanie i szybsze odzyskiwanie sprawności po krytycznych zdarzeniach.

Zaufali nam:

American Red Cross

Parliament | Parlement Canada

Greater Manchester Police

Civil Nuclear Constabulary

BlackBerry | Cybersecurity

3. Zabezpiecz swoje dane na urządzeniach firmowych i osobistych za pomocą BlackBerry UEM, zapewniając szczegółową kontrolę zasad i widoczność potrzebną do zabezpieczenia wszystkich punktów końcowych, poprawy stanu bezpieczeństwa i zgodności z wymogami regulacyjnymi.
Zaufali nam:

Gartner Peer Insights Customers' Choice 2023

Evides waterbedrijf

Grand River Hospital – Advancing Exceptional Care

UNISON – the public service union

4. Rozszerz swój wewnętrzny zespół ds. bezpieczeństwa dzięki CylanceGUARD (XDR), światowej sławy analitykom ds. cyberbezpieczeństwa BlackBerry, za ułamek czasu i kosztów budowy własnego Centrum Operacji Bezpieczeństwa.
Zaufali nam:

Cyber Security Excellence Awards – Winner 2023

Blue Bird Group

RG

5. Ogranicz dostęp do poufnych informacji dzięki CylanceEDGE (ZTNA), natywnemu dla chmury rozwiązaniu BlackBerry Zero Trust, które umożliwia bezpieczną pracę z dowolnego miejsca dla organizacji każdej wielkości.
Zaufali nam:

Cyber Security Excellence Awards – Winner 2023

Granite State credit union

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