LEWIATAN

Warszawa, 2 marca 2021 r.
KL/96/67/ED/2021

Uwagi Konfederacji Lewiatan do wytycznych EROD 01/2021 w sprawie przykładów dotyczących wymogu powiadomień o naruszeniu danych (uwagi przedstawiono do wskazanych punktów wytycznych)

2. Ochrona przed oprogramowaniem ransomware: rozważamy przypadek zdarzenia niekryminalnego rozumianego jako kwalifikacja incydentu w wyniku usterki technicznej leżącej po stronie administratora. Zdaniem Konfederacji Lewiatan rozwiązaniem powinno być wydanie rekomendacji dotyczących zasad postępowania w awariach technicznych o różnej skali.

2.20. Pojęcie "risk to the rights and freedoms of natural persons" jest zbyt ogólne. W praktyce zastanawiamy się czy:

1) sam dostęp do konta jest naruszeniem ww. praw/wolności;

2) kwestia potencjalności - czy ważna jest sama potencjalność problemu dostępności do konta czy przykładowo możemy ustalić, że wśród usterkowych konta nie było zgłoszonych żadnych problemów od *userów*, a tym samym założyć, że w praktyce problem się nie pojawił.

Naszym zdaniem konieczne jest doprecyzowanie ryzyka przez rekomendację bądź przez przykładowe wskazanie konkretnych sytuacji.

2.5 Środki organizacyjne i techniczne służące zapobieganiu/łagodzeniu skutków ataku ransomware: przypominamy, że lista zalecanych środków nie powinna być obowiązkowa. To administrator powinien podejmować decyzje jakie środki wdrożyć w odniesieniu do analizy ryzyka.

3.4. 70: Rekomendacja w tej ogólnikowej formie może spowodować efekt kuli śniegowej - przyjęcie założenia, że kryptografia, hashowanie ma być robione jako *by design* i *by default*. Wymagane jest rozwinięcie w jakich sytuacjach oraz w jakich rodzajach sytuacji jest to rekomendowane. Sugerujemy, że powinna powstać rekomendacja kiedy bezwzględnie jest to konieczne, aby mieć punkt odniesienia. Kolejnym problemem jest obieg elektronicznych dokumentów, które powinny być szyfrowane.

Postulujemy, aby szyfrowanie bądź też hashowanie było rozwinięte, przykładowo poprzez katalog kontekstów czy celów przetwarzania, gdzie jest to bezwzględnie wskazane. Samo słowo *"processed"* jest zbyt ogólne i powinno zostać rozwinięte.

4. Ryzyka pochodzenia wewnętrznego: warto podnieść kwestię błędów, które są spowodowane błędem osoby z zewnątrz - usera. Ostatnio UODO nałożył karę na jedną z firm ubezpieczeniowych za wysłanie

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

polisy na błędny adres e-mail podany przez klienta, z wytłumaczeniem, że firma ta powinna przewidywać takie błędy i mieć to zabezpieczone. Ponadto, powinna to potraktować jako incydent. Rekomendujemy, aby wytyczne zawierały rozstrzygnięcie jaką rolę w kwalifikacji incydentu odgrywa przyczynienie się/przyczyna leżąca po stronie *usera*/osoby, której prawa dotyczą.

4.3. 84: Wyłączanie funkcji drukowania ekranu w systemie operacyjnym jako metoda mitygacji ryzyka ludzkiego: zdaniem Konfederacji Lewiatan jest to funkcja bardzo przydatna w normalnej pracy i taka wytyczna jest nieproporcjonalna. Zabraniając tworzenia tzw. printscreena utrudniamy podstawowe funkcjonowanie bez istotnego wzrostu bezpieczeństwa.

6.5. 123: Wyłączanie autouzupełniania podczas wpisywania adresów e-mail: wygeneruje to problemy z literówkami a jednocześnie nie rozwiąże problemu ludzkich błędów, gdyż ręczne wpisywanie adresów email nie oznacza minimalizacji ryzyka błędu.

Z poważaniem,

Maciej Witucki
Prezydent Konfederacji Lewiatan

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS