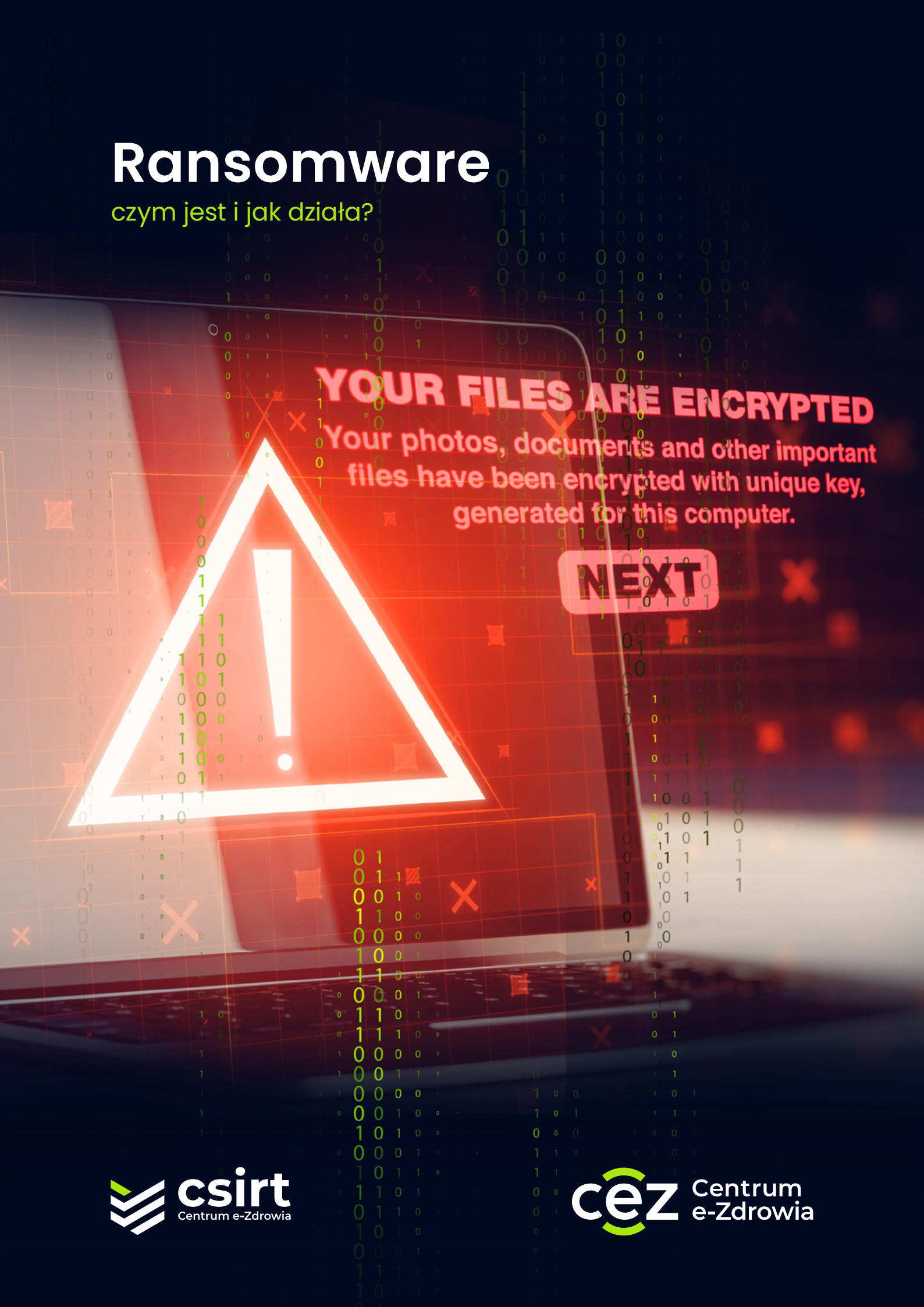
Ransomware

czym jest i jak działa?



csirt
Centrum e-Zdrowia

cez Centrum e-Zdrowia

Ransomware to rodzaj malware czyli szkodliwego oprogramowania, który blokuje dostęp do danych w celu wymuszenia okupu. Po zainfekowaniu systemu pliki zostają zaszyfrowane, a użytkownik otrzymuje komunikat z żądaniem zapłaty w zamian za klucz deszyfrujący. Dodatkowo, często przed zaszyfrowaniem, dane są wykradane, aby szantażować ich właściciela. Przestępcy grożą ich opublikowaniem, jeśli okup nie zostanie zapłacony.

Tego typu ataki są zazwyczaj starannie zaplanowane. Cyberprzestępcy wybierają moment i sposób działania tak, by maksymalnie sparaliżować ofiarę, niezależnie od tego, czy jest to firma, instytucja publiczna czy osoba prywatna. Ma to szczególne znaczenie w sektorze ochrony zdrowia, gdzie konsekwencjami może być utrata życia lub zdrowia przez pacjentów. Stosowane algorytmy szyfrowania są na tyle zaawansowane, że bez oryginalnego klucza odzyskanie danych jest praktycznie niemożliwe. Ofiara musi więc wybierać między utratą plików a ryzykownym spełnieniem żądań przestępców w nadziei na ich odzyskanie.

Warto podkreślić, iż nie należy ulegać szantażowi i dokonywać płatności. Takie działania mogą zostać uznane za wspieranie działalności przestępczej i nie dają żadnej gwarancji odzyskania danych. Nie dają również pewności, że dane nie zostaną opublikowane. Ransomware najczęściej dostaje się do systemu przez luki w zabezpieczeniach, szkodliwe linki oraz załączniki przesyłane pocztą elektroniczną, brak aktualizacji, słabe hasła i zabezpieczenia dostępu zdalnego. Dlatego tak istotne są działania prewencyjne, które prezentujemy poniżej.

01. Jak przygotować się na potencjalny atak?

→ Opracuj plany reagowania i przeprowadzaj okresowo symulacje incydentów (np. w formie gier decyzyjnych).

→ Twórz regularne kopie zapasowe (zgodnie z zasadą 3-2-1):

- minimum trzy egzemplarze kopii danych, na dwóch różnych nośnikach, jeden przechowywany w formie offline odseparowanej od infrastruktury organizacji.

→ Testuj regularnie odzyskiwanie danych z backupów.

→ Zarządzaj procesem aktualizacji:

- monitoruj środowisko pod kątem wdrożonych wersji oraz dostępnych aktualizacji,
- staraj się automatycznie aktualizować oprogramowanie oraz systemy (priorytetowo krytyczne łatki), pamiętając o zachowaniu ciągłości działania,
- określ stałe „okna czasowe" na instalację aktualizacji,
- przygotuj procedurę wycofywania wadliwych wersji.

→ Wprowadź proces zarządzania uprawnieniami:

- ogranicz uprawnienia dla poszczególnych użytkowników,
- stosuj zasadę najmniejszych uprawnień,
- dokumentuj wszelkie zmiany uprawnień,
- ogranicz dostęp do kont uprzywilejowanych (powinny być one udostępnione tylko dla wybranych administratorów).

→ Stosuj uwierzytelnianie wieloskładnikowe (MFA):

- dla wszystkich użytkowników – ze szczególnym uwzględnieniem kont administracyjnych,
- dla dostępu zdalnego (VPN).

→ Wprowadź rozwiązania typu NGAV/EDR/XDR do ochrony stacji roboczych.

→ Stosuj segmentację sieci:

- izoluj systemy krytyczne,
- twórz dedykowane VLANy (w zależności od roli pełnionej przez urządzenia znajdujące się w danej podsieci),
- stosuj rozwiązania klasy IDS/IPS.

→ Regularnie edukuj użytkowników w zakresie phishingu i cyberzagrożeń.

→ Zbieraj, monitoruj i analizuj logi z wykorzystaniem SIEM, UEBA.

→ Wprowadź politykę Application Whitelisting aby uruchamiać tylko zweryfikowane i zaaprobowane przez dział IT aplikacje.

- Stosuj zasadę domyślnego blokowania portów USB i kontroluj nośniki wymienne, aby zapobiec nieautoryzowanemu wprowadzaniu złośliwego oprogramowania.
- Przeprowadzaj regularne testy penetracyjne i audyty konfiguracji.
- Określ, jak długo i w jakiej formie przechowywane są kopie zapasowe oraz prowadź szczegółowy rejestr operacji na kopiach.
- Zapewnij zasilanie awaryjne (UPS, generatory).

02. Jak wykryć wskaźniki trwającego ataku?

- Monitoruj alerty z narzędzi klasy EDR/NGAV o nietypowym zachowaniu aplikacji.
- Śledź anomalie w ruchu sieciowym (NDR/NTA) oraz próby nawiązywania połączeń do C2 (serwerów Command and Control).
- Obserwuj nagłe zmiany w harmonogramach backupów (wyłączanie/uszkodzenia).
- Kontroluj logowania administracyjne – szczególnie o nietypowych porach i lokalizacjach.
- Korzystaj z systemów honeypot/deception (fałszywe konta administracyjne).
- Wykrywaj zmiany w konfiguracji zabezpieczeń i wyłączenia narzędzi antywirusowych.
- Monitoruj aktywność i alerty związane z próbami dostępu do zasobów wrażliwych.
- Zbieraj i analizuj logi dotyczące uruchomienia makr, aby wiedzieć, kiedy i kto je uruchomił.
- Obserwuj zmiany w konfiguracjach.

03. Jak postępować w przypadku ataku ransomware?

- Natychmiast izoluj zaatakowane urządzenia od sieci (zdalna izolacja przez EDR, banowanie MAC adresów, fizyczne odpięcie od sieci lokalnej).
- Nie wyłączaj z prądu żadnych urządzeń.
- Zawiadom zespół reagowania na incydenty (SOC, CSIRT).
- Powiadom osoby decyzyjne, w tym dyrekcję, o incydencie.
- Przeprowadź szybką ocenę zakresu ataku (identyfikacja zainfekowanych maszyn i danych).
- Przygotuj się do odbudowy infrastruktury obejmującej serwery, urządzenia sieciowe (firewalle, routery, koncentratory VPN) oraz stacje robocze
- Każde z urządzeń będące w zaatakowanej sieci potraktuj jak skompromitowane.
- Rozpocznij odzyskiwanie danych z kopii zapasowych na osobnych urządzeniach (ogranicz się do niezbędnych plików i baz danych).
- Nie odtwarzaj obrazów systemów ani ich konfiguracji, ponieważ mogą one być już skompromitowane.
- Dokonaj analizy powłamaniowej (digital forensics) i przygotuj raport z przyczyn ataku.
- Poinformuj klientów, partnerów oraz wymagane organy regulacyjne (UODO, policja, CERT).
- Po zakończeniu incydentu wprowadź zalecenia z analizy, popraw procedury bezpieczeństwa oraz zaktualizuj plany reagowania.
- Zapewnij łatwe i szybkie kanały zgłaszania incydentów (dedykowany e-mail, telefon do SOC lub działu IT).
- Przygotuj komunikaty kryzysowe oraz procedury ich szybkiego publikowania i dystrybucji.
- Zarchiwizuj wszystkie logi z czasu incydentu oraz maksymalny zakres logów przed wystąpieniem incydentu, na zewnętrznych nośnikach lub do izolowanego środowiska, aby nie zostały nadpisane lub usunięte przez atakujących.
- Zabezpiecz próbki ransomware i artefakty ataku do analizy. Przechowuj próbki w bezpiecznym, odizolowanym środowisku.