

OCENA RYZYKA A ODPORNOŚĆ SIECI I SYSTEMÓW INFORMATYCZNYCH NA INCYDENTY CYBERBEZPIECZEŃSTWA



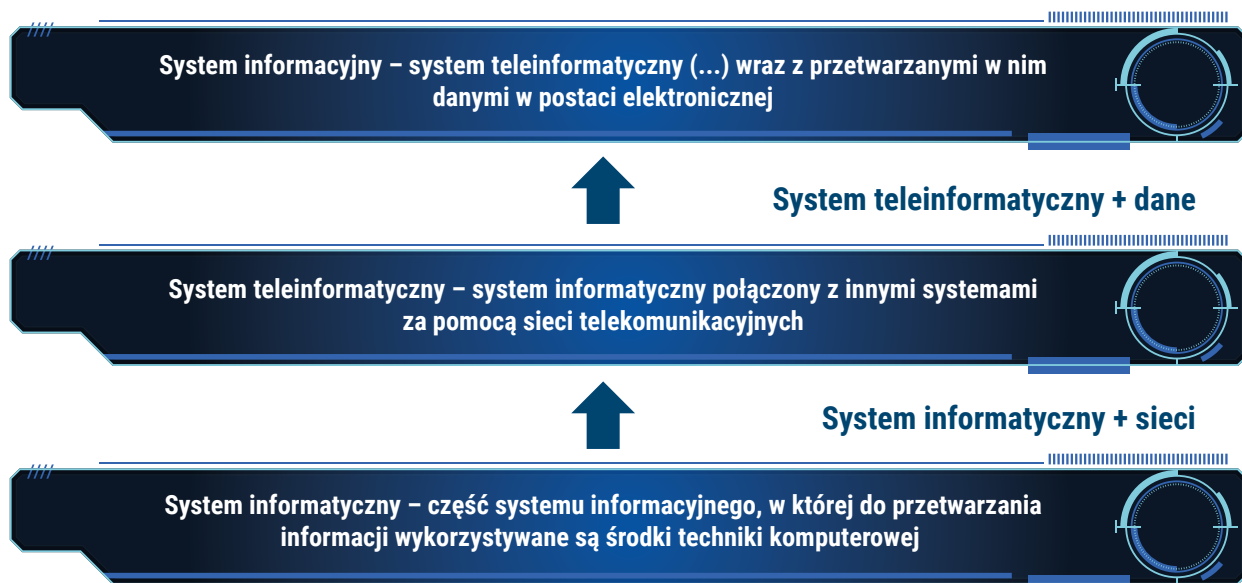
MICHAŁ ŁONIEWSKI

Kierownik Wydziału
Rozwoju Technicznego
Przewodniczący Zespołu Zadaniowego
ds. Cyberbezpieczeństwa
Departament Innowacji i Rozwoju
Urząd Dozoru Technicznego

BEZPIECZEŃSTWO SIECI I SYSTEMÓW INFORMATYCZNYCH ZDEFINIOWANE JEST W DYREKTYWIE NIS 2 2022/2555/UE JAKO: „ODPORNOŚĆ SIECI I SYSTEMÓW INFORMATYCZNYCH, PRZY DANYM POZIOMIE ZAUFANIA, NA WSZELKIE ZDARZENIA, KTÓRE MOGĄ NARUSZYĆ DOSTĘPNOŚĆ, AUTENTYCZNOŚĆ, INTEGRALNOŚĆ LUB POUFNOŚĆ PRZECHOWYWANYCH, PRZEKAZYWANYCH LUB PRZETWARZANYCH DANYCH LUB USŁUG OFEROWANYCH PRZEZ TE SIECI I SYSTEMY INFORMATYCZNE LUB DOSTĘPNYCH ZA ICH POŚREDNICTWEM” [1].

Definicja systemu informatycznego (a także teleinformatycznego, który połączony jest z innymi za pomocą sieci telekomunikacyjnych) mówi natomiast, że **SYSTEM INFORMATYCZNY** to ta część systemu informacyjnego, w której do przetwarzania informacji wykorzystywane są środki techniki komputerowej [3].

Definicja ta obejmuje również przemysłowe systemy sterowania (*Industrial Control Systems, ICS*) występujące wszędzie tam, gdzie mamy do czynienia z fizyczną realizacją procesów produkcyjnych, przesyłowych, magazynowych czy transportu bliskiego. Podstawowe definicje przedstawia rys. 1.



Rys. 1. Definicje systemów informacyjnych

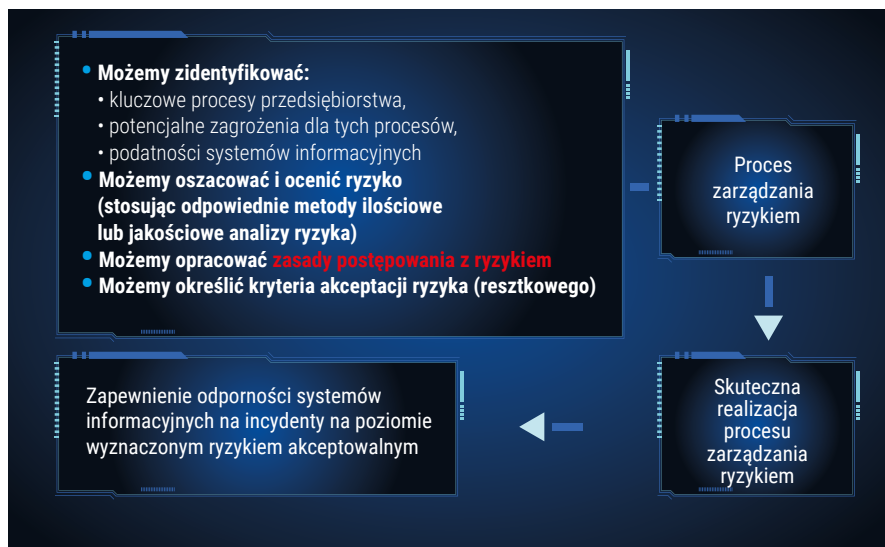
CZYM ZATEM JEST ODPORNOŚĆ SYSTEMÓW I SIECI INFORMATYCZNYCH?

CZY MOŻEMY Z CAŁĄ PEWNOŚCIĄ STWIERDZIĆ, ŻE NASZE AKTYWA SĄ WYSTARCZAJĄCO BEZPIECZNE I ODPORNE?

Niestety nie, nigdy bowiem nie będziemy pewni, że nasze sieci i systemy mają w danym momencie odpowiedni (wystarczający) poziom bezpieczeństwa i odporności na zagrożenia. Wynika to z faktu, że bezpieczeństwo oraz odporność (sieci i systemów) na incydenty są wartościami niemierzalnymi, występującymi najczęściej jako pojęcia jakościowe.

JAK ZATEM ZWIĘKSZAĆ BEZPIECZEŃSTWO I BUDOWAĆ ODPORNOŚĆ?

Z pomocą przychodzi nam proces zarządzania ryzykiem w organizacji, podczas którego możemy zidentyfikować kluczowe procesy przedsiębiorstwa, potencjalne zagrożenia dla tych procesów (w tym potencjalne incydenty dotyczące sieci i systemów informatycznych) oraz opracować zasady postępowania ze zbyt wysokim ryzykiem materializacji zagrożenia czy konsekwencji. Proces ten przedstawia rys. 2.

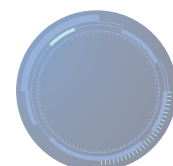
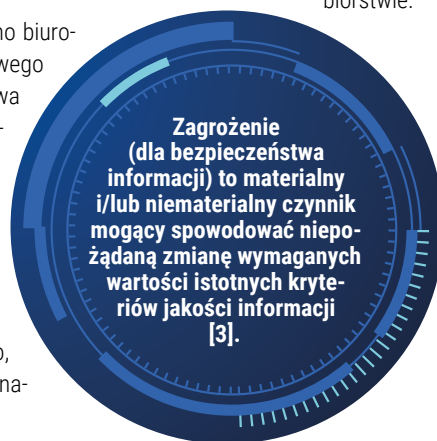
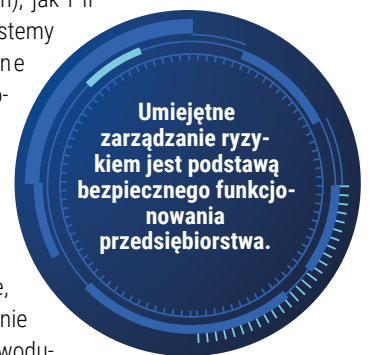


Rys. 2. Zarządzanie ryzykiem a odporność sieci i systemów informatycznych na incydenty

Budowanie odporności sieci i systemów informatycznych zarówno biurowych IT (Information Technology, IT), jak i sterowania przemysłowego OT (Operational Technology, OT) na incydenty cyberbezpieczeństwa jest procesem ciągłym i wynikającym z poziomu ryzyka wystąpienia incydentu (wartości prawdopodobieństwa materializacji zagrożenia i wielkości jego potencjalnych konsekwencji).

Skuteczne prowadzenie procesu zarządzania ryzykiem w przedsiębiorstwie pozwala na zapewnienie odporności sieci i systemów informatycznych na poziomie wyznaczonym ryzykiem zaakceptowanym przez przedsiębiorstwo, np. najwyższe kierownictwo, zarząd. Oznacza to, że odporność naszych sieci i systemów wyznacza poziom ryzyka zaakceptowany przez organizację.

Zarówno atak zdalny (zwany potocznie atakiem hakerskim), jak i fizyczny na systemy informatyczne i sieci definiowane są jako jeden ze sposobów realizacji zagrożenia poprzez nieuprawnione, celowe działanie człowieka powodujące niepożądaną zmianę wymaganych wartości istotnych kryteriów jakości informacji. Zagrożenie natomiast jest pojęciem szerszym i tak powinno być rozpatrywane podczas oceny ryzyka w przedsiębiorstwie.



PODSTAWOWE ELEMENTY PROCESU ZARZĄDZANIA RYZYKIEM

- Prawidłowa identyfikacja kluczowych procesów w przedsiębiorstwie
- Identyfikacja potencjalnych zagrożeń dla tych procesów
- Identyfikacja podatności sieci i systemów informatycznych
- Szacowanie i ocena ryzyka (z wykorzystaniem odpowiednich metod ilościowych i jakościowych analizy ryzyka)
- Opracowanie zasad postępowania ze zbyt wysokim ryzykiem (unikanie ryzyka, transfer ryzyka, kontrola ryzyka, retencja/zatrzymanie ryzyka)
- Określenie kryteriów jego akceptacji

Należy mieć na uwadze, że zarządzanie ryzykiem cyberbezpieczeństwa, zdarzeń zagrażających przedsiębiorstwu jako potencjalne incydenty cyberbezpieczeństwa, występuje jako wymaganie i dobra praktyka.

A. WYMAGANIE

- w obowiązującej jeszcze ustawie o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. [7] na podstawie dyrektywy NIS 2016/1148/UE (dotyczy operatorów usług kluczowych) [2]
- w dyrektywie NIS 2 2022/2555/UE [1] (dla podmiotów kluczowych, w tym administracji publicznej oraz podmiotów ważnych – znacznie szerszy zakres niż w dyrektywie NIS 2016/1148/UE); listę sektorów kluczowych i ważnych przedstawia tab. 1

B. DOBRA PRAKTYKA w normach wskazanych w uzasadnieniu do obowiązującej ustawy o KSC.

- PN-EN ISO/IEC 27001:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania (obecnie: PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania) [5]
- PN-EN ISO 22301:2020-04 Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania [4]

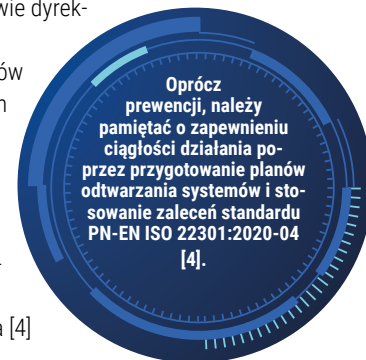


Tabela 1. Sektory podmiotów kluczowych i ważnych według dyrektywy NIS 2 (kolor czerwony – zmiany w stosunku do dyrektywy NIS; kolor zielony – brak zmian w stosunku do dyrektywy NIS)

Sektory podmiotów kluczowych	Sektory podmiotów ważnych
Energetyka (energia elektryczna, system ciepłowniczy lub chłodniczy, ropa naftowa, gaz, wodór)	Usługi pocztowe i kurierskie
Transport (lotniczy, kolejowy, wodny, drogowy)	Gospodarowanie odpadami
Bankowość	Produkcja (wyroby medyczne i wyroby medyczne do diagnostyki in vitro, produkty komputerowe, elektroniczne i optyczne; sprzęt elektryczny; maszyny i urządzenia; pojazdy samochodowe, przyczepy i naczepy; pozostały sprzęt transportowy)
Infrastruktura rynków finansowych	Produkcja, wytwarzanie i dystrybucja chemikaliów
Opieka zdrowotna	Produkcja, przetwarzanie i dystrybucja żywności
Woda pitna	Dostawcy usług cyfrowych
Ścieki	Badania naukowe
Infrastruktura cyfrowa	
Zarządzanie usługami ICT (między przedsiębiorstwami)	
Podmioty administracji publicznej	
Przestrzeń kosmiczna	

Ocena ryzyka powinna być przeprowadzana cyklicznie, co najmniej raz w roku, oraz po każdej istotnej planowanej lub występującej niespodziewanie zmianie w działalności przedsiębiorstwa. Prawidłowo przeprowadzona ocena definiuje konieczność wdrożenia brakujących bądź rozbudowy istniejących zabezpieczeń / środków ochronnych organizacyjnych, fizycznych i technicznych. Przykładowe środki ochronne przedstawia rys. 3.

Zabezpieczenia organizacyjne (wspierające skuteczność zabezpieczeń fizycznych i technicznych)

- Polityka bezpieczeństwa
- Zintegrowany system zarządzania
- Cykliczne audyty bezpieczeństwa
- SOC wewnętrzny i/lub zewnętrzny (ang. Security Operation Center)
- Edukacja i budowanie świadomości pracowników
- Weryfikacja dostawców

Zabezpieczenia fizyczne (obiektów, łączy i urządzeń)

- Ochrona osobowa - straż, firma ochroniarska
- Służby wewnętrzne
- Ogrodzenia, przegrody budowlane
- Bunkry
- Drzwi, zamki, kraty
- Sejfy, szafy pancerne

Zabezpieczenia techniczne

- Obiektów, łączy i urządzeń
- systemy ppoż/pgaz.
- systemy sygnalizacji napadu i włamania
- systemy kontroli dostępu
- systemy rejestracji czasu pracy
- systemy nadzoru wizyjnego
- Sprzętowo-programowe - produkty realizujące funkcje ochronne
- segmentacja sieci (model Purdue, DMZ, VLAN)
- monitorowanie sieci (SIEM, IDS/IPS, SOAR)
- komunikacja jednokierunkowa (data diodes)
- firewall
- oprogramowanie antywirusowe
- szyfrowanie transmisji danych oraz plików
- bezpieczne metody uwierzytelniania
- regularne kopie bezpieczeństwa
- terminowe aktualizacje
- ograniczone wykorzystanie pamięci przenośnych



Rys. 3. Przykłady zabezpieczeń/środków ochronnych

W przypadku oceny ryzyka sieci i systemów informatycznych sterowania i kontroli (OT) warto skorzystać z opracowanych dla tego sektora standardów. Popularną serią standardów przemysłowych, wywodzącą się z tej samej amerykańskiej organizacji normalizacyjnej ISA (International Society of Automation), w której opracowano serię standardów dotyczącą bezpieczeństwa funkcjonalnego dla przemysłu procesowego (seria IEC 61511), jest seria **IEC 62443 (ISA-99) Security for Industrial Automation and Control Systems**.

Zaletą serii jest uzupełnienie zagadnień bezpieczeństwa funkcjonalnego *safety* o zagadnienia dotyczące cyberbezpieczeństwa *security* (*No safety without security*). W polskim wydaniu arkusza normy **PN-EN IEC 62443-3-2:2021-03 Bezpieczeństwo w systemach sterowania i automatyki przemysłowej -- Część 3-2: Ocena ryzyka w bezpieczeństwie i projektowaniu systemu** [6] znajdziemy przydatne informacje dotyczące oceny ryzyka sieci i systemów sterowania przemysłowego, budynkowego, transportowego, wodno-kanalizacyjnego czy też medycznego.

Podstawowe etapy oceny ryzyka dla systemów sterowania, opisane w standardzie:

- identyfikacja rozważanego systemu (System Under Consideration,

SUC) – zdefiniowanie ocenianego systemu w ramach systemu automatyki i sterowania przemysłowego (Industrial Automation and Control Systems, IACS),

- przeprowadzenie wstępnej (zgrubnej) oceny ryzyka cyberbezpieczeństwa,
- podzielenie SUC na strefy i kanały – grupowanie aktywów w strefy i kanały, przy czym priorytetem jest zidentyfikowanie tych aktywów, które mają wspólne wymagania dotyczące bezpieczeństwa, i umożliwienie identyfikacji wspólnych środków bezpieczeństwa (zabezpieczeń) wymaganych do ograniczenia ryzyka,
- wykonanie szczegółowej oceny ryzyka cyberbezpieczeństwa dla każdej strefy i kanału oraz określenie docelowego poziomu bezpieczeństwa SL-T (Security Level-Target) dla każdej strefy i kanału,
- udokumentowanie zaktualizowanych wymagań cyberbezpieczeństwa dla szczegółowego projektu (specyfikacja wymagań cyberbezpieczeństwa – Cybersecurity Requirements Specifications, CRS).

Standard wskazuje ponadto, aby podczas oceny ryzyka szczególną uwagę poświęcić systemom bezpieczeństwa, systemom automatyki zabezpieczającej, przyrządowym systemom bezpieczeństwa SIS (Safety Instrumented Systems), systemom łączności bezprzewodowej, systemom połączonym bezpośrednio do punktów końcowych sieci internet, systemom będących interfejsem do IACS, ale zarządzanych przez zewnętrzne podmioty (w tym systemom zewnętrznym) i urządzeniom mobilnym.

Z uwagi na poziom ryzyka wynikający z pozostającej zawsze większej bądź mniejszej możliwości wystąpienia incydentu (ryzyko resztkowe / szczątkowe) każde przedsiębiorstwo powinno być przygotowane na jego wystąpienie. Kluczowym procesem, obok procesu zarządzania ryzykiem w organizacji, jest zatem proces zarządzania incydentami, a w szczególności proces ich obsługi. Należy przy tym pamiętać, że całkowita eliminacja występowania incydentów nie jest możliwa, a proces zarządzania ryzykiem ich wystąpienia i konsekwencji powinien być stałym elementem działalności organizacji.

Literatura:

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS).
3. Liderman K. (2017). Bezpieczeństwo informacyjne. Nowe wyzwania. Warszawa: Wydawnictwo Naukowe PWN.
4. PN-EN ISO 22301:2020-04 Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania.
5. PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
6. PN-EN IEC 62443-3-2:2021-03 Bezpieczeństwo w systemach sterowania i automatyki przemysłowej -- Część 3-2: Ocena ryzyka w bezpieczeństwie i projektowaniu systemu.
7. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 oraz z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655).