



Ministerstwo
Cyfryzacji



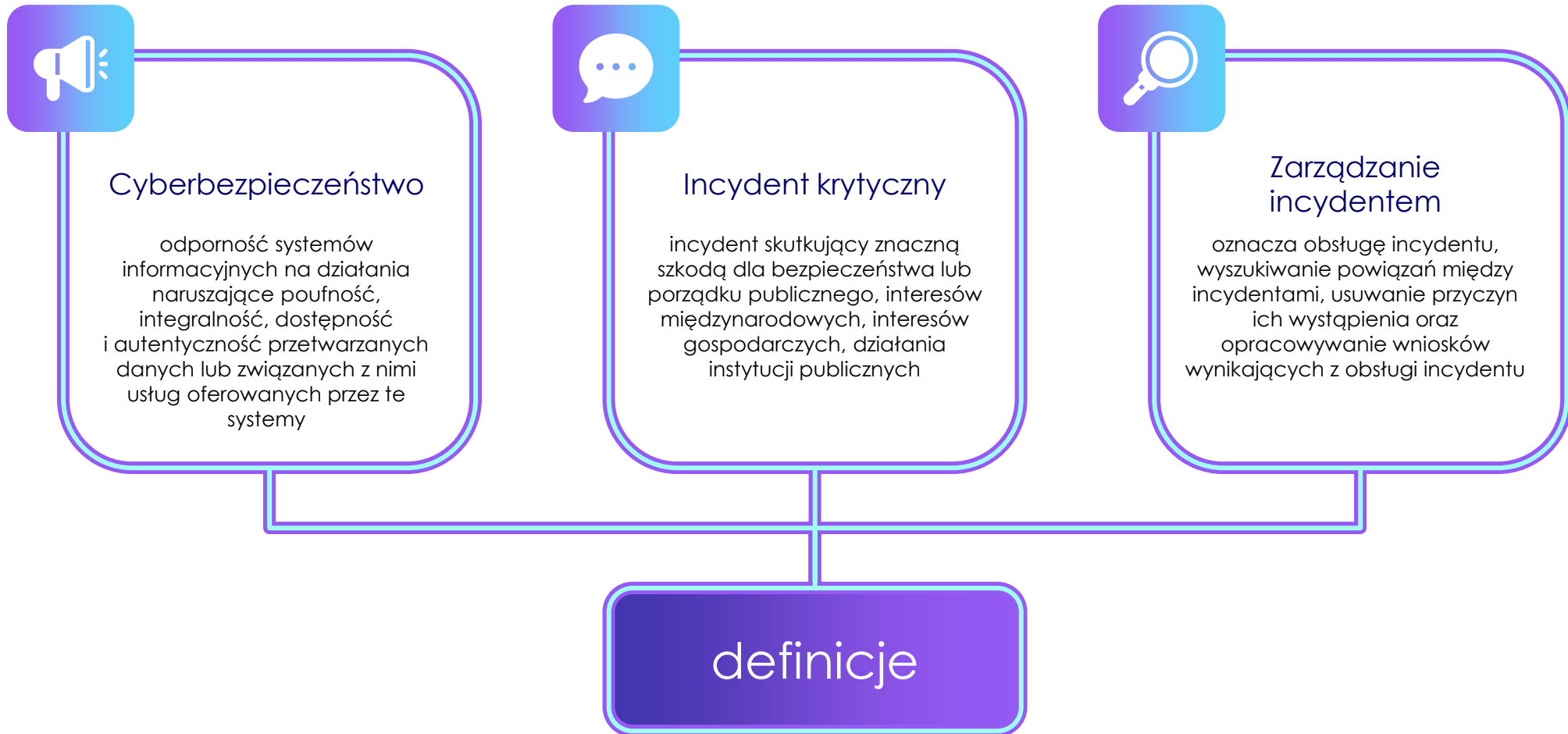
Ministerstwo
Finansów

CYKL UMIEJĘTNOŚCI CYFROWE

Jak dbać o cyberhigienę w pracy?

Warszawa, 12 października 2023 r.

Podstawowe definicje cyberbezpieczeństwa



Atrybuty cyberbezpieczeństwa

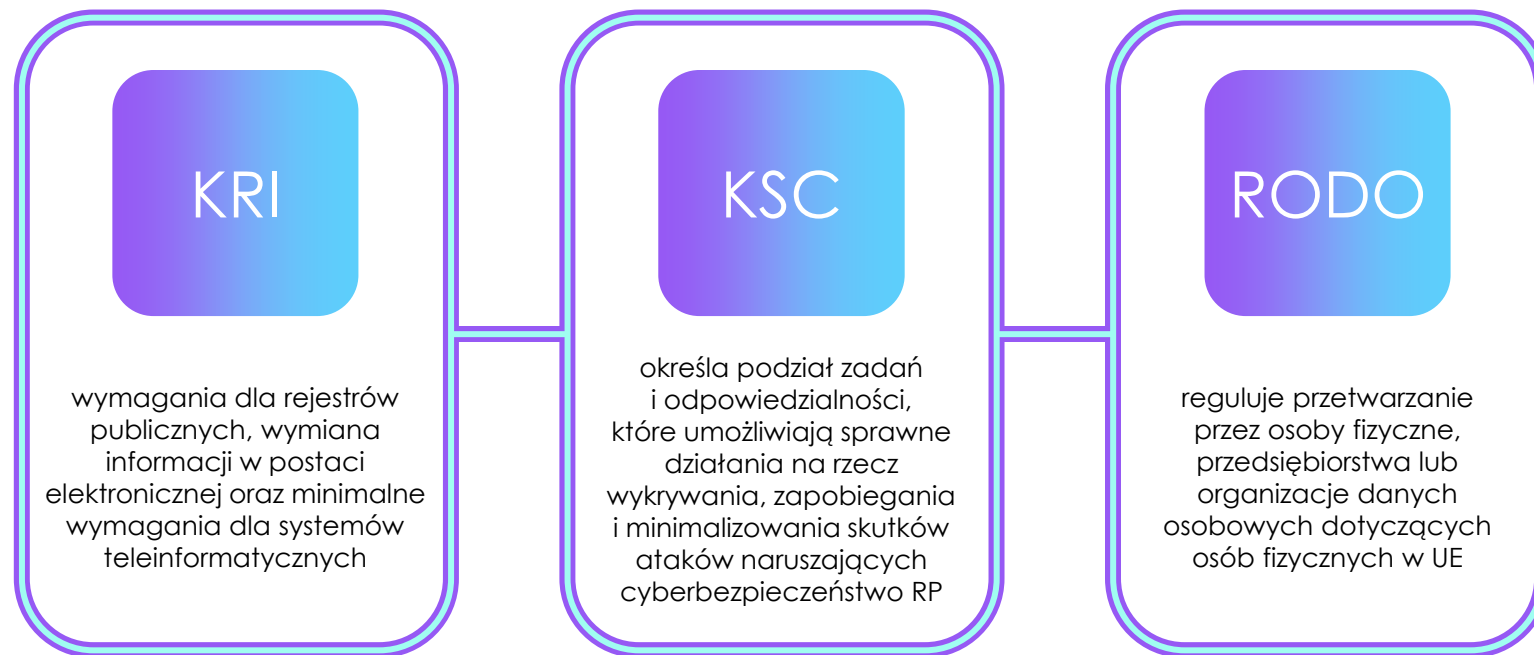


Bezpieczeństwo informacji

podstawą zachowania cyberbezpieczeństwa jest
zarządzanie bezpieczeństwem informacji

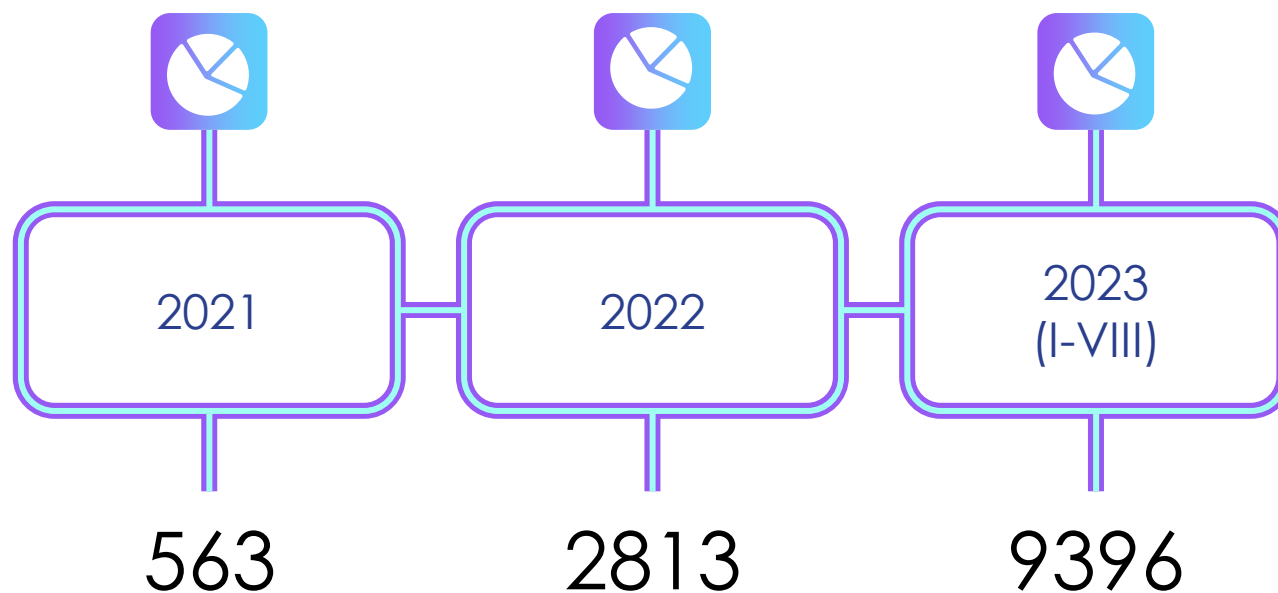
obejmuje polityki, procedury, standardy i wytyczne
dotyczące ochrony informacji oraz określa role
i odpowiedzialności pracowników w zakresie
bezpieczeństwa informacji

Regulacje

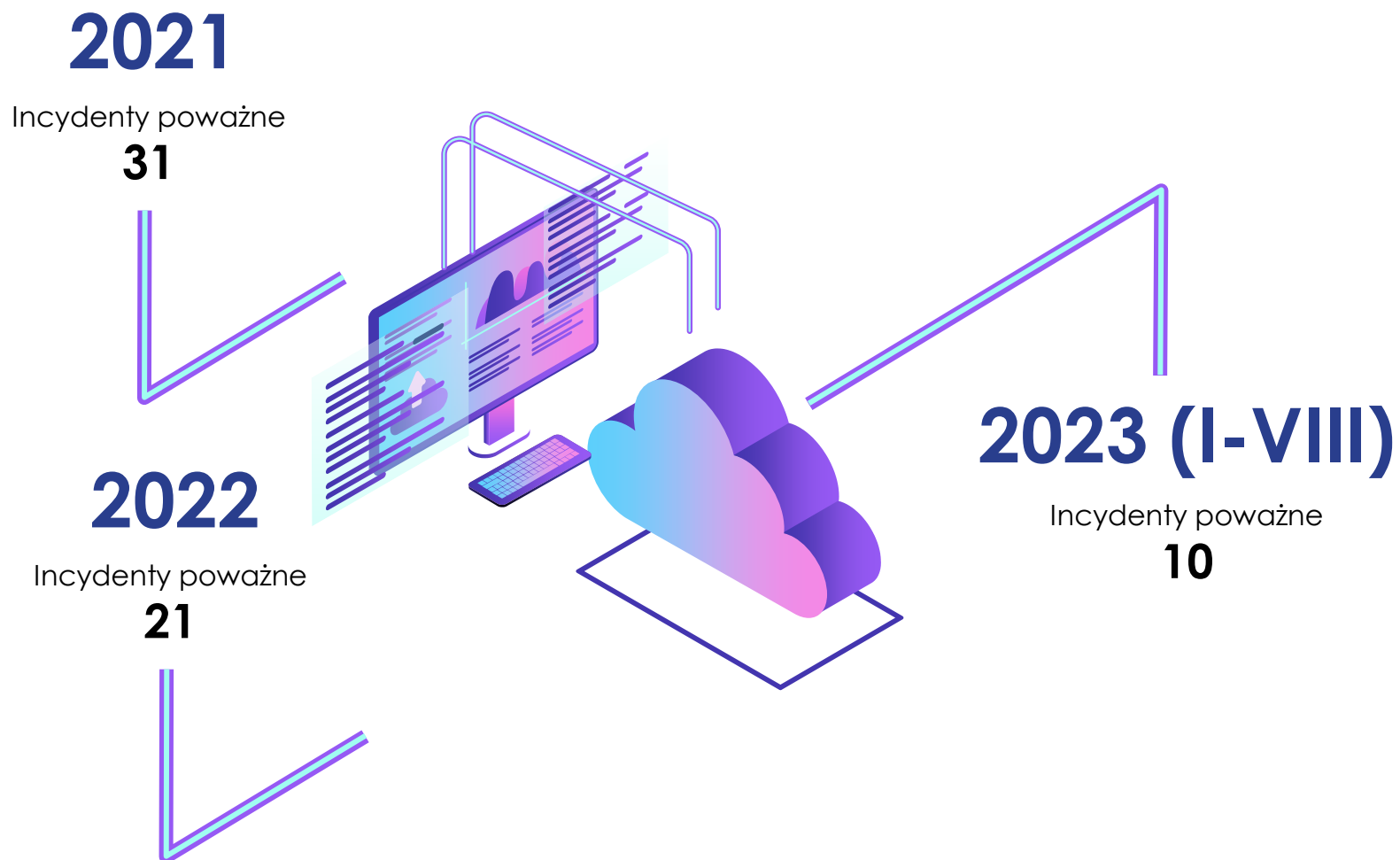


Statystyki

Incydenty obsługiwane przez CERT Polska - infrastruktura rynków finansowych



Statystyki



Projekt Artemis

Artemis jest kluczowym narzędziem wykorzystywanym przez NASK w celu ochrony infrastruktury krytycznej w Polsce. System ten umożliwia szybkie wykrywanie i reagowanie na zagrożenia cybernetyczne, co jest niezwykle istotne w obliczu rosnącej liczby ataków i coraz bardziej zaawansowanych technik stosowanych przez przestępców. Dzięki Artemis, NASK może wspierać organy rządowe, instytucje publiczne i prywatne przedsiębiorstwa w zapewnieniu bezpieczeństwa ich sieci komputerowych i danych. NASK zgłasza administratorom znalezione podatności



Projekt Artemis

W ramach projektu Artemis od początku stycznia do końca września 2023 r. łącznie przeskanowano:

- 521 domen banków;
- ok. 2,3 tys. subdomen banków.

Łącznie zgłoszono **ok. 1,9 tys. podatności** lub błędnych konfiguracji, w tym 111 wiążących się z wysokim, ok. 1,3 tys. średnim i 474 - niskim zagrożeniem. Przynajmniej jedną podatność/błędną konfigurację wykryto w 846 przeskanowanych domenach/subdomenach.

Wśród wykrytych problemów najczęściej było przypadków korzystania z nieaktualnego oprogramowania, np. z wtyczek do **WordPressa (758)** oraz błędnie skonfigurowanych mechanizmów weryfikacji nadawcy **poczty e-mail (564)**.

Uwaga! Skanowanie jest automatyczne, dlatego też powyższe liczby mogą zawierać duplikaty lub odnosić się do sytuacji, w których w rzeczywistości podatność nie występuje, ponieważ np. wykryto niepoprawnie skonfigurowane SSL/TLS w domenę, która w praktyce nie jest używana.

CSIRT NASK rozpoczął skanowanie OUK, wśród których znajdują się duże banki. Wyniki tego skanowania w postaci zbiorczych statystyk poznamy w IV kwartale br

Źródła ataków



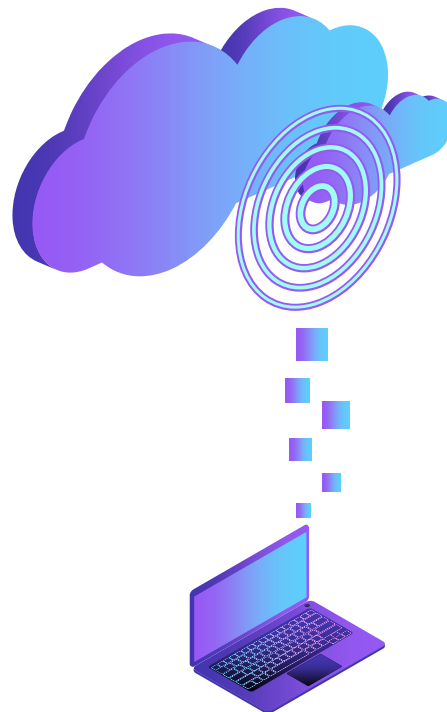
Cyberprzestępcy

Osoby lub grupy, które przeprowadzają ataki hakerskie w celu zdobycia dostępu do informacji lub usług



Osoby wew. organizacji

Pracownicy lub kontrahenci, którzy posiadają dostęp do systemów informatycznych organizacji, mogą próbować zdobyć nieuprawniony dostęp do poufnych informacji



Obce rządy

Państwa lub grupy wywiadowcze - te podmioty przeprowadzają ataki w celu pozyskania wrażliwych informacji związanych z bezpieczeństwem narodowym lub gospodarczym



Aktywiści

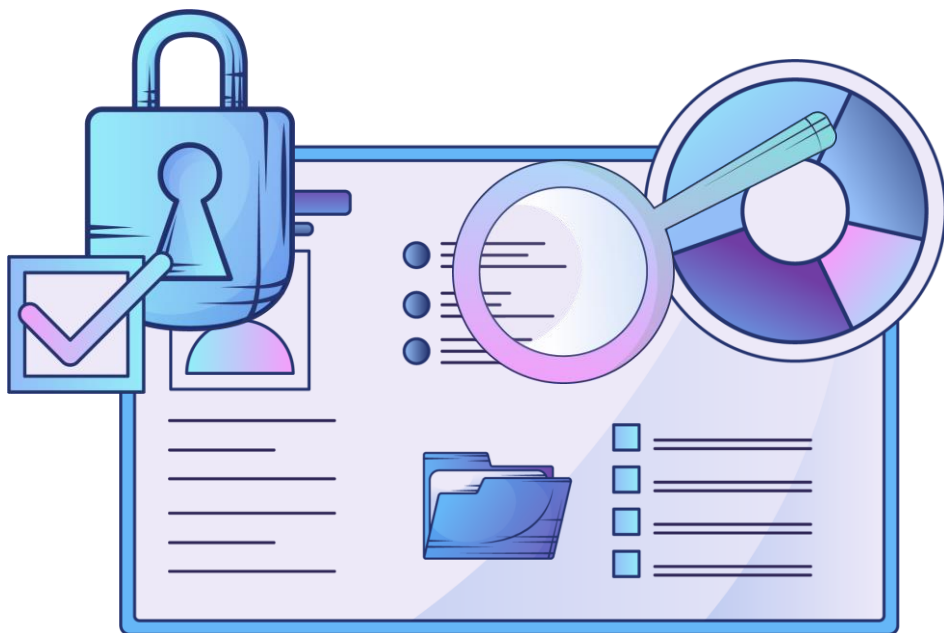
Osoby lub grupy, które wykorzystują cyberprzestrzeń do celów politycznych lub ideologicznych

Stopień CHARLIE–CRP

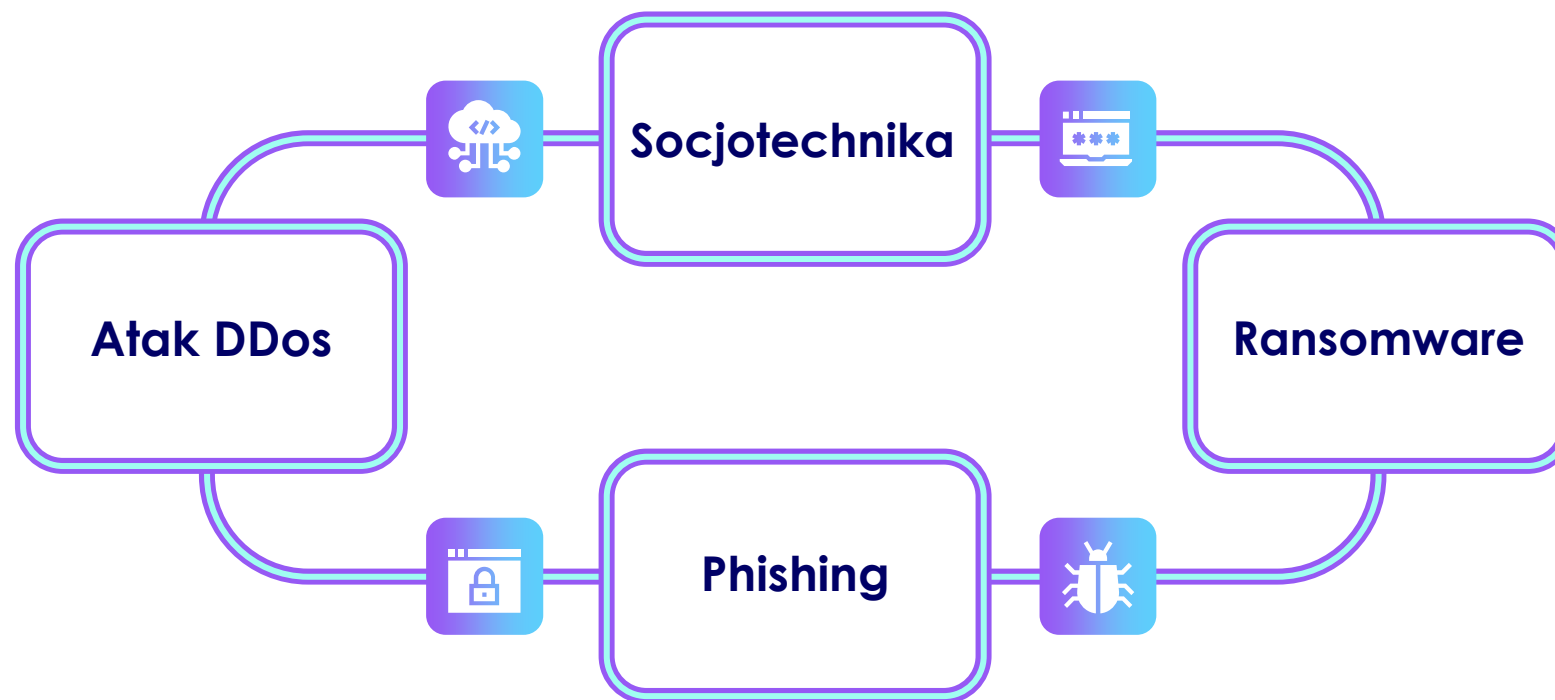
Stopień dotyczy bezpieczeństwa cyberprzestrzeni jest trzecim z czterech stopni alarmowych określonych w ustawie o działaniach antyterrorystycznych.

Stopień ten jest wprowadzany w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym w cyberprzestrzeni albo uzyskania wiarygodnych informacji o planowanym zdarzeniu.

Ten stopień alarmowy obejmuje cały kraj. Dotyczy podmiotów publicznych i infrastruktury krytycznej.

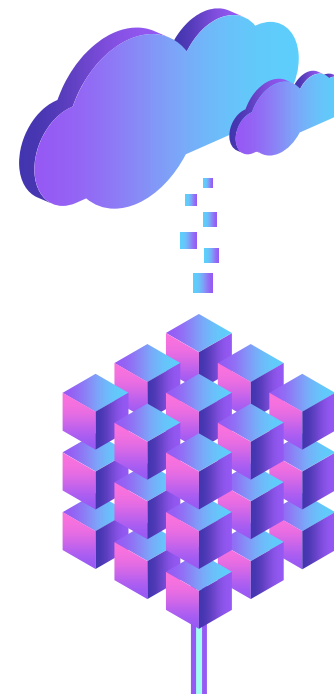


Rodzaje ataków



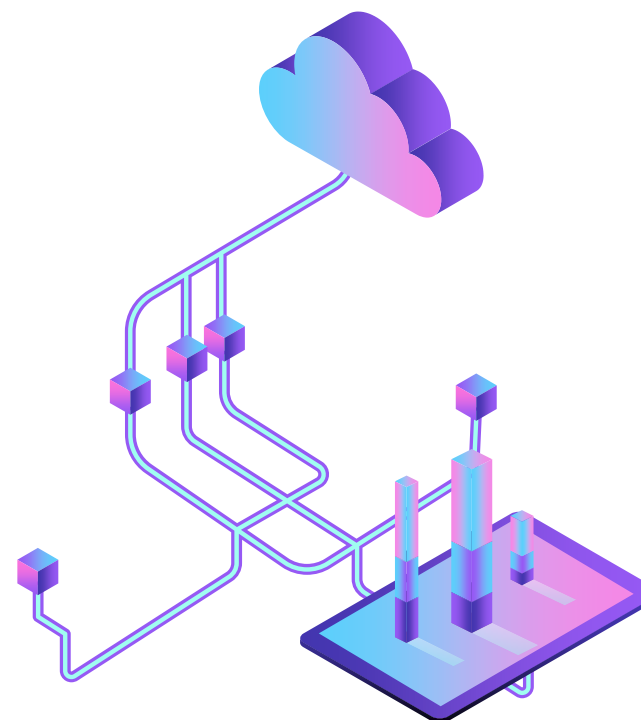
Aatak DDos

atak polegający na przeciążeniu serwera przez wysłanie ogromnej ilości żądań, co powoduje niedostępność usługi



Socjotechnika

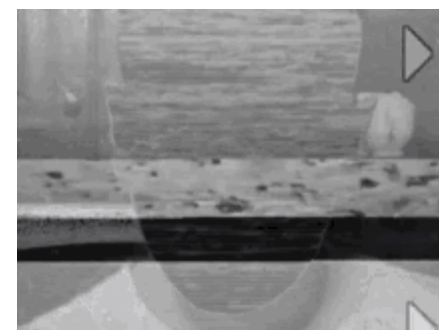
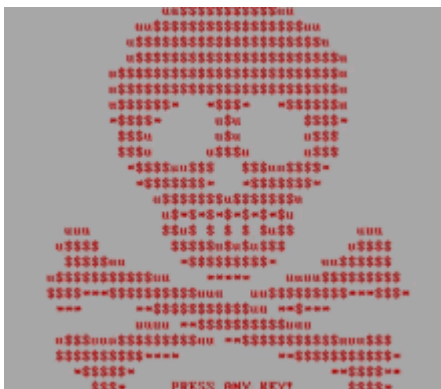
atak polegający
na manipulowaniu ludźmi,
aby uzyskać od nich poufne
informacje



Ransomware

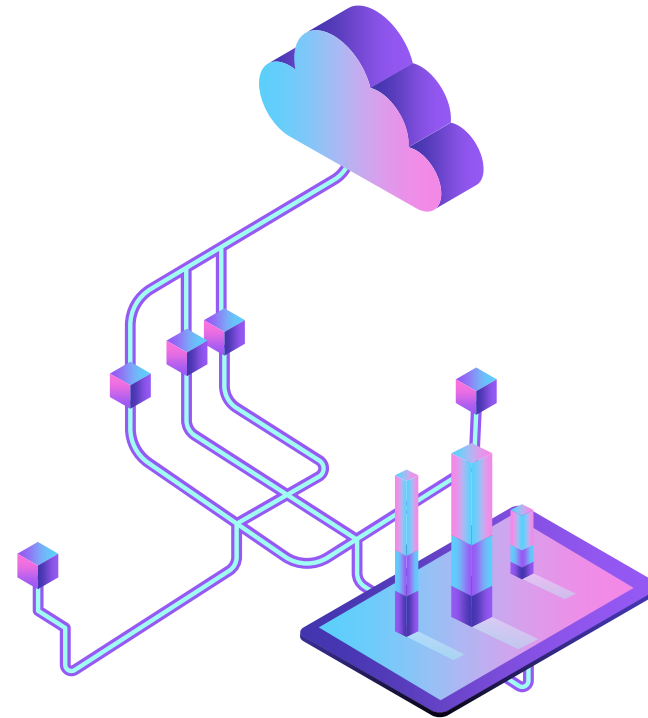
oprogramowanie szantażujące,
które zaszyfrowuje dane
użytkownika, żądając okupu za ich
odszyfrowanie





Phishing

polega na próbie pozyskania
wrażliwych danych,
np. uwierzytelniających
do systemów bankowych lub
portali społecznościowych



Przykład phishingu

From: POCZTA.ONET.PL <bogusla[redacted]@onet.pl>

Sent: Sunday, February 19, 2023 4:56 PM

To: [redacted]

Subject: 🌐🔴 Ostrzeżenie o dezaktywacji konta

Szanowny Kliencie

Twoja skrzynka pocztowa została wybrana do dezaktywacji i zostanie trwale usunięta z bazy poczty onet. Musisz podjąć PILNE działanie bez wahania w ciągu najbliższych 24 godzin, aby uniknąć dezaktywacji konta, a także zaktualizować swoje konto.

[Kliknij tutaj](#) TERAZ pobierz nasz nowy system kont Onet z naszego serwera pocztowego.

Powiadomienie to jest generowane automatycznie przez serwer bezpieczeństwa poczty Onet Poczta.

Z poważaniem, usługi Onet Poczta.PL - Administrator(C) 2023 [ONET.PL](#)

[ONET.PL](#)

<https://fdfghjklkjhgf.weebly.com>

Źródło: <https://cert.pl/posts/2023/04/phishing-webmail/>

Metoda typosquatting

Link poprawny	Link sfalszowany	Wytłumaczenie
allegro.pl	allegro.pl	duża litera i jako mała litera l
gettinbank.pl gov.pl	qettinbank.pl qov.pl	mała litera Q jako mała litera G
dotpay.pl	clotpay.pl	małe litery C i L jako mała litera d
mbank.pl	rnbank.pl	małe litery R i N jako litera mała m

Rodzaje phishingu

Aatak ukierunkowany na KONKRETNEGO adresata czyli

SPEARPHISHING

wyłudzenie DANYCH w trakcie rozmowy telefonicznej to

VISHING

Przykłady ataków

Hakerzy zaatakowali portal podatki.gov.pl. Nie można było złożyć ePIT-ów

Cyberprzestępcy zablokowali dostęp do rządowej serwisu podatki.gov.pl. Od kilku dni na rosyjskich stronach trwały rozmowy na temat ataku na polskie serwery.

Publikacja: 20.02.2023 08:41



Foto: PAP/Darek Deimanowicz

p.mal

Uwaga na fałszywe SMS-y dot. nadpłaty lub niedopłaty PIT

Publikacja: 2022.03.31 12:32 Aktualizacja: 2022.03.31 12:36 Źródło: Ministerstwo Finansów

- Krajowa Administracja Skarbowa nie wysyła do podatników żadnych wiadomości SMS ws. nadpłaty lub niedopłaty w podatku
- Nadpłatę bądź niedopłatę wynikającą z rozliczenia rocznego można sprawdzić w serwisie e-Urząd Skarbowy na podatki.gov.pl lub w urzędzie skarbowym.



Resort finansów nie jest nadawcą wiadomości SMS, które trafiają do podatników, a w treści wiadomości znajduje się link prowadzący rzekomo do konta urzędu skarbowego lub numer telefonu komórkowego, pod którym będzie można skontaktować się z (fałszywym) pracownikiem skarbowki.

Wiadomości są próbą wyłudzenia danych. Nadpłatę bądź niedopłatę wynikającą z rozliczenia rocznego można sprawdzić w serwisie e-Urząd Skarbowy na podatki.gov.pl lub w urzędzie skarbowym.

Przestrzegamy i apelujemy o ostrożność

Serwis eFaktura padł ofiarą podwójnego ataku hakerskiego

🕒 21 września 2022, 15:00

ALERT

Rządowy serwis eFaktura.gov został zhakowany – podaje portal Niebezpiecznik. Sprawcami były prawdopodobnie dwie niezależne grupy hakerskie. Póki sytuacja nie zostanie opanowana, lepiej być ostrożnym przy używaniu rzeczonoego serwisu.

CSIRT KNF

UWAGA NA FAŁSZYWE REKLAMY!

The image is a composite showing a social media post on the left and a website on the right, connected by a red arrow. The social media post is from 'Wiadomości ze świata' and features a headline about gas prices and a photo of a queue at a government office. The website is 'baltic pipe' and features a headline about earning money on European gas, a photo of a gas meter, and a registration form.

Wiadomości ze świata
Sponsorowane

Jak uniknąć opłaty gazu?
Patrz artykuł na stronie internetowej

**PRZEDWYBORCZY DODATEK GAZOWY
DAJE MOŻLIWOŚĆ UNIKNĄĆ OPŁATY GAZU**

UZYSKAJ MOŻLIWOŚĆ KLIKAJĄC NA LINK

NALORIM.COM
Wyłącznie dla Polaków
Otrzymaj możliwość

Dowiedz się...

baltic pipe

Zarabiaj na europejskim gazie nawet do €10 000

Polska została partnerem projektu Baltic Pipe, postanowiliśmy dać możliwość naszym obywatelom przyłączyć się do nas i zarabiać pasywnie na akcjach.

Zarejestruj się!

Twoje imię
Twoje nazwisko
example@gmail.com
512345678

Założ darmowe konto

GAZ system PARTNERZY PROJEKTU

Dlaczego jest to korzystne dla zwykłych obywateli

Co musisz teraz zrobić, aby zacząć zarabiać na BALTIC PIPE?

Źródło: https://twitter.com/CSIRT_KNF

CSIRT KNF

UWAGA NA FAŁSZYWE STRONY!

poland-gov.com

gov.pl

Sprawdź swoje punkty karne (usługa online)

Proszę wprowadzić numer rejestracyjny pojazdu lub numer mandatu.

informacja

(np. WU A 123 or #000000)

POTWIERDZAĆ

ADRES

ul. Królewska 27
00-060 Warszawa
NIP 5213621697
Regon 145881488

poland-gov.com/order

gov.pl

Sprawdź swoje punkty karne (usługa online)

mandat za wykroczenia drogowe szczegóły

1. Numer faktury	PL0338A4213
2. data kary	30/09/2023
3. rodzaj naruszenia	przekroczenie prędkości w obszarze zabudowanym
4. kwota	150 zł
5. data ważności	03/10/2023
6. organ karzący	polski urząd transportu

POTWIERDZAĆ

poland-gov.com/paym

gov.pl

Sprawdź swoje punkty karne (usługa online)

Posiadasz Karty

Numer Karty

0000 0000 0000 0000

VISA

Data Ważności

MM/YY

Kod Bezpieczeństwa (CVV)

123

POTWIERDŹ PŁATNOŚĆ

ADRES

ul. Królewska 27
00-060 Warszawa
NIP 5213621697

NIEBEZPIECZNA DOMENA

Źródło: https://twitter.com/CSIRT_KNF

CSIRT KNF

UWAGA NA FAŁSZYWE POSTY!



Źródło: https://twitter.com/CSIRT_KNF

Bezpieczne hasło

- ☐ Hasło nie powinno być takie samo jak nazwa użytkownika lub część tej nazwy,
- ☐ Hasło nie powinno być imieniem nikogo z naszych najbliższych,
- ☐ Hasło nie powinno zawierać danych osobowych Twoich lub Twojej rodziny,
- ☐ Nie używaj sekwencji kolejnych liter, liczb lub innych znaków.



- ☐ Nie używaj pojedynczego wyrazu dowolnego języka pisanego normalnie lub wspak
- ☐ Nie używaj więcej niż 3 kolejnych znaków na klawiaturze
- ☐ Nie używaj oczywistych wyrażeń, takich jak wpuscmnie
- ☐ Hasło powinno mieć co najmniej 14 znaków

Siła hasła

LICZBA ZNAKÓW	TYLKO MAŁE LITERY	PRZYNAJMNIEJ JEDNA DUŻA LITERA	PRZYNAJMNIEJ JEDNA DUŻA LITERA + CYFRA	PRZYNAJMNIEJ JEDNA DUŻA LITERA + CYFRA + SYMBOL
1	NATYCHMIAST	NATYCHMIAST	-	-
2	NATYCHMIAST	NATYCHMIAST	NATYCHMIAST	-
3	NATYCHMIAST	NATYCHMIAST	NATYCHMIAST	NATYCHMIAST
4	NATYCHMIAST	NATYCHMIAST	NATYCHMIAST	NATYCHMIAST
5	NATYCHMIAST	NATYCHMIAST	NATYCHMIAST	NATYCHMIAST
6	NATYCHMIAST	NATYCHMIAST	NATYCHMIAST	NATYCHMIAST
7	NATYCHMIAST	NATYCHMIAST	1 MINUTA	6 MINUT
8	NATYCHMIAST	22 MINUTY	1 GODZINA	8 GODZIN
9	2 MINUTY	19 GODZIN	3 DNI	3 TYGODNIE
10	1 GODZINA	1 MIESIĄC	7 MIESIĘCY	5 LAT
11	1 DZIEŃ	5 LAT	41 LAT	400 LAT
12	3 TYGODNIE	300 LAT	2 000 LAT	34 000 LAT

Tworzenie bezpiecznego hasła

Użycie frazy

Wybierz łatwy do zapamiętania cytat, piosenkę lub frazę i użyj pierwszej litery z każdego słowa. Używaj liter różnej wielkości. Pamiętaj, aby uwzględnić również liczby i symbole, zastępując nimi litery lub całe słowa. Słowa „Mam dwadzieścia lat” można na przykład zapisać jako M@m2dzie\$ciA!4T. Możesz skorzystać z poniższych reguł, żeby je odpowiednio zmodyfikować, choć pamiętaj, że możesz zastosować swoje zasady:

- zamień a na @
- zamień s na \$
- zamień spację na %
- zamień małe „o” na 0
- zamień i na !

Np. Damian Oh zapisz jako D@m!an%Oh.



Złożoność hasła

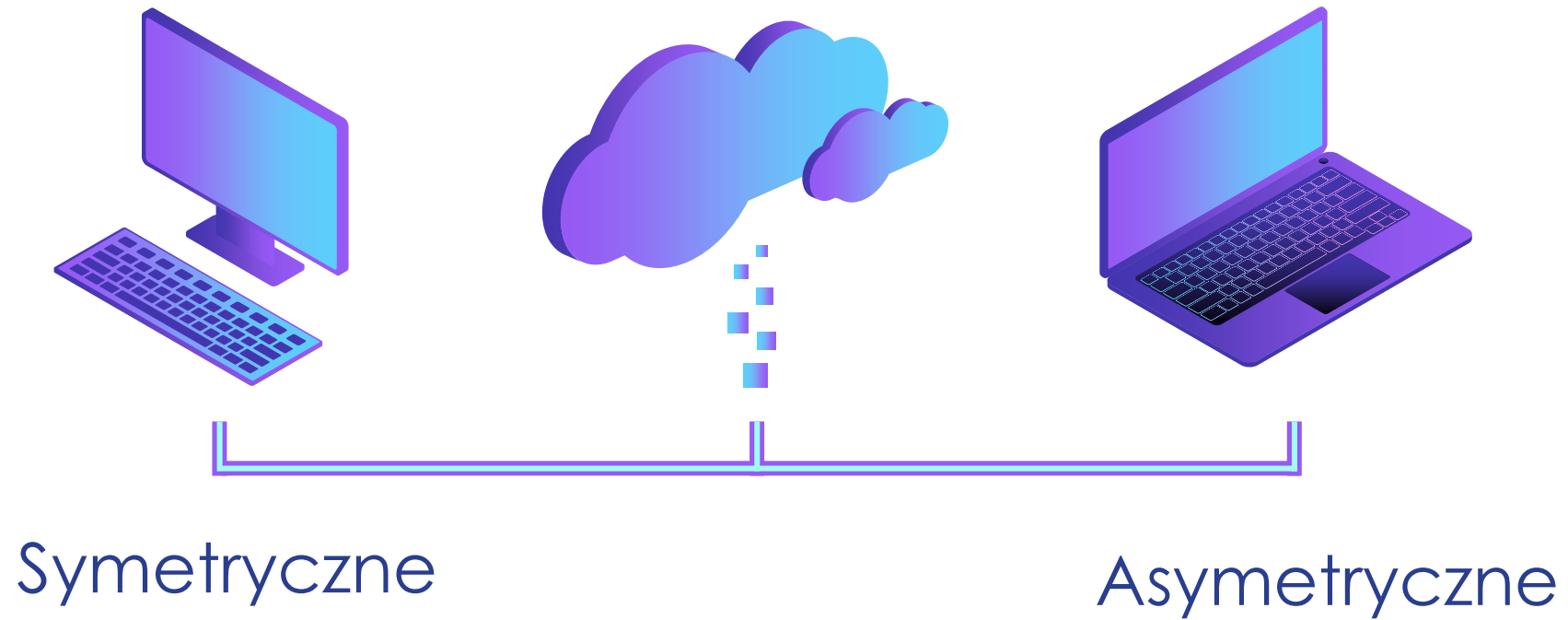
Hasło powinno zawierać co najmniej jeden znak z każdej z następujących grup:

- małe litery
- duże litery
- liczby
- znaki specjalne

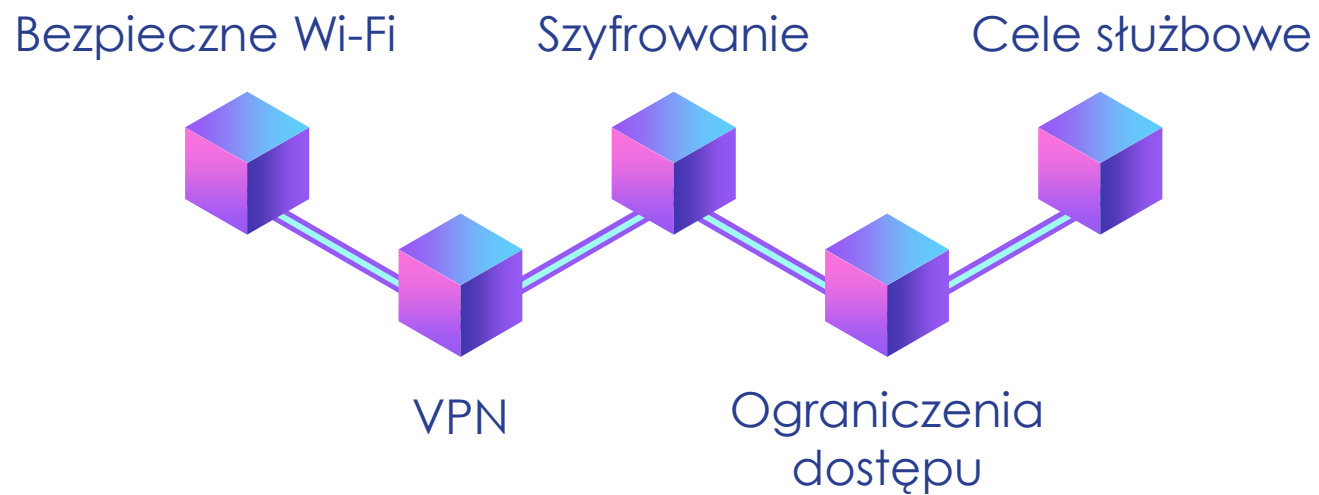
Jak zwiększyć bezpieczeństwo?



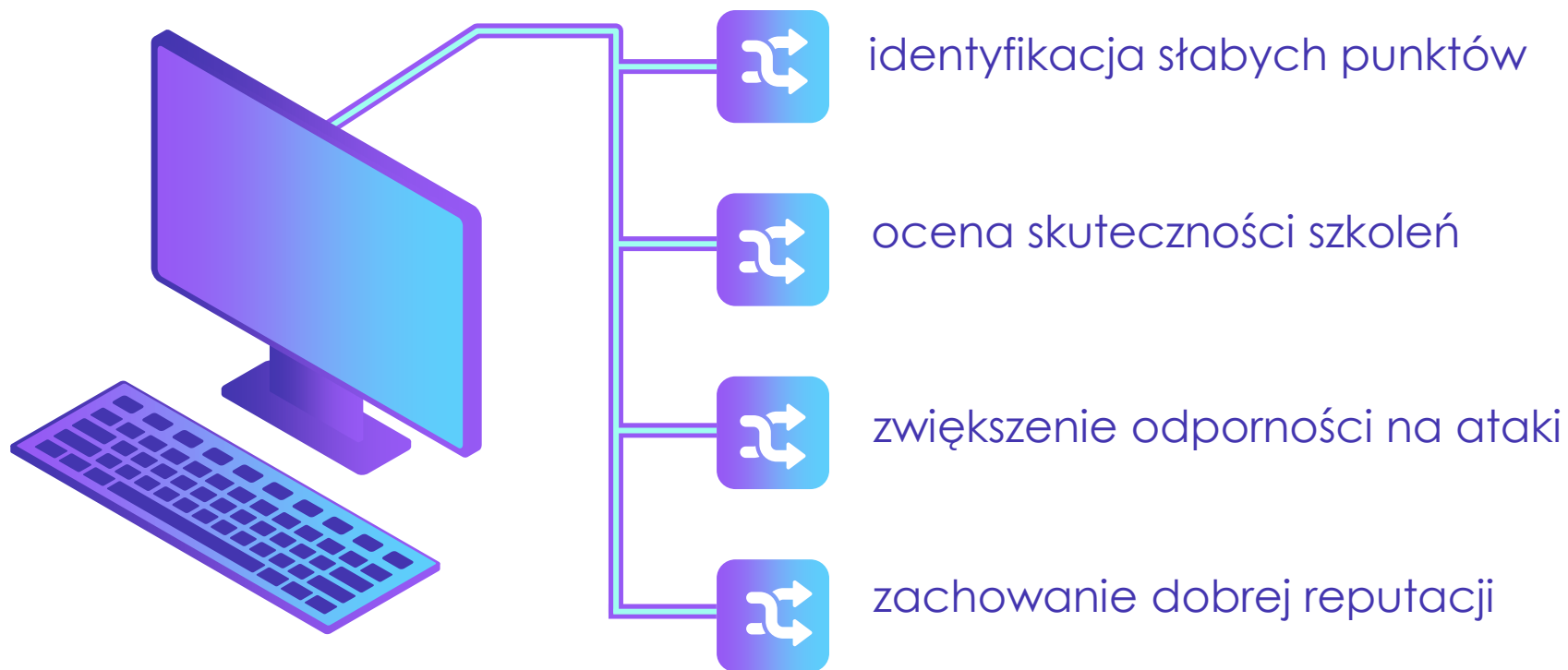
Szyfrowanie



Bezpieczeństwo pracy zdalnej



Zalety testów phishingowych



Dobre praktyki

- ❑ Oddzielanie spraw służbowych i prywatnych: poczty, serwisów społecznościowych, usług chmurowych,
- ❑ Indywidualne konta na urządzeniu, szczególnie w przypadku urządzeń wykorzystywanych przez kilka osób,
- ❑ Aktualizacja systemu operacyjnego oraz aplikacji (automatyczne aktualizacje),
- ❑ Instalacja oprogramowania z zaufanych źródeł,
- ❑ Szyfrowanie urządzeń (dysków zewnętrznych, pamięci USB),
- ❑ Szyfrowanie komunikacji oraz przegląd korespondencji: usuwanie wiadomości ze skrzynki odbiorczej oraz wysłanych, ustawianie automatycznego kasowania wiadomości w komunikatorach,
- ❑ Nie korzystanie z niezauważalnych nośników: dyski zewnętrzne, pamięci i urządzenia USB,
- ❑ Korzystanie z własnych ładowarek sieciowych,
- ❑ Korzystanie z filtrów ekranowych.



Wyzwania



Zgłaszanie incydentu

Zgodnie art. 11 ust. 3 pkt 1 UKSC jeżeli w sektorze został ustanowiony sektorowy zespół cyberbezpieczeństwa OUK zgłoszenie incydentu poważnego
**przekazuje CSIRT krajowemu
i jednocześnie zespołowi sektorowemu.**

Jak zgłosić incydent?



Służbowo

Jeżeli incydent wystąpił w służbowej sieci lub urzędzeniu, niezwłocznie powiadom o tym zespół IT lub przełożonego i podążaj za ich wskazówkami.

Wyznaczona osoba do kontaktu ma obowiązek zgłaszania incydentów do CSIRT NASK.

W przypadku wykrycia nietypowego zachowania systemu informacyjnego, wskazującego na możliwość wystąpienia incydentu cyberbezpieczeństwa czy groźnego cyberataku najważniejsza jest **szybkość reakcji**.

Każda organizacja powinna mieć ustaloną politykę związaną z obsługą incydentu.

Jak zgłosić incydent?



Prywatnie

Jeżeli incydent wystąpił w twojej prywatnej sieci lub urzędzeniu zgłoś incydent jako osoba fizyczna poprzez:

- stronę internetową <https://incydent.cert.pl/>
- na adres cert@cert.pl
- sms - 799 448 084 (nie dzwonić)

Bezpłatne szkolenia online

- ❑ Szkolenia 100 - cyberhigiena dla każdego – podstawowe porady i najlepsze praktyki z zakresu cyberbezpieczeństwa dla wszystkich pracowników.
- ❑ Szkolenia 200 - dla kadry zarządzającej, pracowników działów IT – podstawy prawne krajowego systemu cyberbezpieczeństwa, obowiązki podmiotów wynikające z ustawy, procedury zgłaszania incydentów, najczęstsze cyberzagrożenia i sposoby ochrony.
- ❑ Szkolenia 300 - warsztaty dla specjalistów IT, programistów, osób zarządzających cyberbezpieczeństwem w podmiotach krajowego systemu cyberbezpieczeństwa - prezentacje projektów wspierających cyberbezpieczeństwo w organizacji, analizy rodzajów cyberataków, reagowanie na incydenty, zgłaszanie incydentów, profilaktyka cyberbezpieczeństwa w organizacji, szkolenia specjalistyczne dotyczące zastosowania konkretnych rozwiązań prowadzone przez partnerów technologicznych.

<https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen>



Baza wiedzy

gov.pl

Serwis Rzeczypospolitej Polskiej

Zaloguj

Strona główna

Rada Ministrów

Kancelaria Premiera

Ministerstwa

Urzędy, instytucje i placówki RP

Usługi dla obywatela

Usługi dla przedsiębiorcy

Usługi dla urzędnika

Usługi dla rolnika

Profil zaufany

Baza wiedzy

Serwis Służby Cywilnej

Сайт для громадян України

-Serwis dla obywateli Ukrainy

Baza wiedzy

Cyberbezpieczeństwo

Aktualności

Aktualności

Dla każdego - cyberhigiena

Dla profesjonalistów

Dla samorządów

Narodowe Standardy Cyberbezpieczeństwa

Program Współpracy w Cyberbezpieczeństwie

CyberEdukacja

Szkolenia

Komunikator

Subskrypcje cyberwiadomości

Najczęściej zadawane pytania

Uważaj na fałszywe próby o szybki przelew

1 nie otwieraj podejrzanych

2 nie klikaj w linki z nieznanych źródeł

3 nie udawaj się pracownikiem i nie udawaj, że pracownik

CSIRT NASK ostrzega przed oszustwem „na rekrutację”

W kolejnym spotu kampanii edukacyjno-informacyjnej Ministerstwo Cyfryzacji i NASK podpowiadają jak chronić się przed oszustwami na szybkie przelewy.

OSZUSTWO

Partnerzy Programu Współpracy w Cyberbezpieczeństwie (PWCyber) dyskutowali o przyszłości programu podczas V Forum Cyberbezpieczeństwa w ramach XXXII Forum Ekonomicznego w Karpaczu.

Źródło: <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>

 Ministerstwo
Cyfryzacji

Szkolenie cz. 2

Cyberbezpieczeństwo 2.0: Nowe podejście do zarządzania ryzykiem i audytu w cyberprzestrzeni.

- ❑ Zarządzanie ryzykiem: identyfikacja i ocena ryzyka cyberataków dla organizacji.
- ❑ Kontrola i audyt: omówienie procesów audytu cyberbezpieczeństwa i jakie kontrole należy przeprowadzać, aby zabezpieczyć systemy informatyczne przed atakami.

14 grudnia 2023 r.



Ministerstwo
Cyfryzacji



Ministerstwo
Finansów

Dziękuję za uwagę!

Warszawa, 12 października 2023 r.



Ministerstwo
Cyfryzacji
