ZARZĄDZENIE NR 22/2022

BURMISTRZA SURAŻA

z dnia 27 maja 2022 r.

w sprawie wprowadzenia regulaminu zgłaszania, obsługi i zarządzania incydentami cyberbezpieczeństwa

Na podstawie art. 22 ust. 1, ust. 2 i ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r (Dz.U. z 2020 r. poz. 1369 t.j ze zm.) zarządzam, co następuje:

§ 1. Wprowadzam do użytku służbowego regulamin zgłaszania, obsługi i zarządzania incydentami cyberbezpieczeństwa, która stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2. Zobowiązuję wszystkich pracowników Urzędu Miejskiego w Surażu oraz Kierowników i Dyrektorów jednostek organizacyjnych Gminy Suraż do zapoznania się i przestrzegania postanowień zawartych w dokumencie, o którym mowa w § 1.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

mgr inż. Henryk Łapiński

Załącznik nr 1
do Zarządzenia nr 22 / 2022
Burmistrza Suraża
z dnia 27 maja 2022 r.

Regulamin

zgłaszania, obsługi i zarządzania incydentami cyberbezpieczeństwa

Spis treści

Rozdział 1

Postanowienia ogólne, definicje

1. Procedura zgłaszania, obsługi i zarządzania incydentami związanymi z cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Gminy.
2. Podstawą prawną do opracowania i wdrożenia dokumentu jest:
   a) art. 22 ust. 1, ust. 2 i ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r (Dz.U. z 2020 r. poz. 1369 t.j ze zm.).
3. Definicje
   a) cyberbezpieczeństwo - odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy,
   b) incydent - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo,
   c) incydent krytyczny - incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV,
   d) incydent poważny - incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej,
   e) incydent istotny - incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151",
   f) incydent w podmiocie publicznym - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny;
   g) zagrożenie cyberbezpieczeństwa - potencjalna przyczyna wystąpienia incydentu,
   h) obsługa incydentu - czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu,
   i) podatność - właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa,
   j) ryzyko - kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji,
   k) szacowanie ryzyka - całościowy proces identyfikacji, analizy i oceny ryzyka,
   l) system informacyjny - system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, 568 i 695), wraz z

przetwarzanymi w nim danymi w postaci elektronicznej,

m) usługa cyfrowa - usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), wymienioną w załączniku nr 2 do ustawy,

n) usługa kluczowa - usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych,

o) zagrożenie cyberbezpieczeństwa - potencjalną przyczynę wystąpienia incydentu,

p) zarządzanie incydentem - obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu,

q) zarządzanie ryzykiem - skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka,

r) CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z siedzibą w Warszawie (01 – 045) przy ul. Kolskiej 12, tel.: 22 380 82 00 tel.: 22 380 82 01; e-mail: nask@nask.pl,

s) Administrator Systemów Informatycznych – osoba odpowiedzialna w Urzędzie za funkcjonowanie systemu(-ów) lub sieci informatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci informatycznych zwany dalej „ASI",

b) osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa – osoba wyznaczona przez podmiot publiczny zgodnie z art. 21 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r (Dz.U. z 2020 r. poz. 1369 t.j ze zm.) - informuje ASI o kontaktach z podmiotami krajowego systemu cyberbezpieczeństwa,

t) Gmina – Gmina Suraż,

u) Burmistrz – Burmistrz Gminy Suraż,

v) Urząd – Urząd Miejski w Surażu ul. 11 Listopada 16, 18-105 Suraż.

Rozdział 2

Podstawowe zasady cyberbezpieczeństwa

1. Należy unikać korzystania z nieznanych urządzeń (publiczne komputery udostępniane w hotelach, bibliotekach, etc.).
2. W systemach operacyjnych, które tego wymagają, niezbędna jest instalacja i regularna aktualizacja oprogramowania antywirusowego.
3. Należy zachować ostrożność podczas pobierania plików z sieci Internet lub otwierania załączników należy zawsze przeczytać uważnie pojawiające się w przeglądarce komunikaty o alertach bezpieczeństwa i nigdy nie ignorować pojawiających się ostrzeżeń dotyczących zagrożeń ceberbezpieczeństwa.
4. Należy unikać połączeń za pośrednictwem niezweryfikowanych sieci (publiczne Wi-Fi).
5. Nie wolno instalować nieznanego oprogramowania otrzymanego pocztą elektroniczną lub pozyskanych z nieznanych lub niezaufanych źródeł.
6. Nigdy nie należy podłączać do komputera nieznanych nośników danych.
7. Nie wolno zezwalać osobom trzecim na manipulowanie urządzeniem mobilnym

lub instalację oprogramowania.

8. Należy korzystać wyłącznie z legalnego oprogramowania pochodzącego ze znanego i zaufanego źródła.
9. Należy regularnie aktualizować posiadany system operacyjny oraz używane aplikacje, szczególności należy aktualizować przeglądarki internetowe, klientów poczty, przeglądarki plików pdf.
10. Nie wolno wyłączać mechanizmów bezpieczeństwa.
11. W zakresie logowanie się do systemów teleinformatycznych zaleca się stosować poniższe zasady dotyczące siły hasła (hasło musi składać się minimum z 8 znaków oraz musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, cyfry lub znaku specjalnego, niedopuszczalne jest używanie tego samego hasła do różnych systemów oraz jego zapisywanie, hasło powinno być regularnie - co 30 dni zmieniane oraz nie może być nikomu udostępniane).

Rozdział 3

Kategorie incydentów

1. Incydent cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Jego przyczyną może być (*Załącznik 1 Lista potencjalnych zagrożeń*):
   a) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych,
   b) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów a także prowadzić do zniszczenia lub utraty danych,
   c) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.
2. Incydenty cyberbezpieczeństwa mogą powodować:
   a) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom,
   b) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji,
   c) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.

Rozdział 4

Zgłaszanie incydentów związanych z cyberbezpieczeństwem przez pracowników Urzędu

1. W przypadku stwierdzenia incydentu krytycznego lub incydentu w podmiocie publicznym pracownik Urzędu niezwłocznie powiadamia o tym fakcie ASI.
2. Zgłoszenie należy potwierdzić szczegółową notatką służbową, którą przekazuje się ASI poprzez swojego bezpośredniego przełożonego lub bezpośrednio do ASI w przypadku pracowników zatrudnionych na samodzielnych stanowiskach.

3. Notatka musi zawierać następujące informacje:
   a. imię i nazwisko osoby zgłaszającej;
   b. stanowisko oraz komórka organizacyjna Urzędu;
   c. dokładne miejsce oraz datę i godzinę wystąpienia incydentu;
   d. ilość osób dotkniętych incydentem;
   e. opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.
4. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

Rozdział 5

Zgłaszanie incydentów związanych z cyberbezpieczeństwem przez jednostki organizacyjne Gminy

1. W przypadku stwierdzenia incydentu krytycznego lub incydentu w podmiocie publicznym przez jednostki organizacyjne Gminy należy niezwłocznie telefonicznie powiadomić o tym fakcie ASI w Urzędzie. W dalszej kolejności fakt ten należy zgłosić mailowo i potwierdzić oficjalnym pismem opatrzonym podpisem kierownika/dyrektora jednostki. Dane kontaktowe ASI są dostępne w sekretariacie Urzędu.
2. W zgłoszeniu należy podać wszystkie informacje zgodnie z treścią art. 23 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 t.j ze zm.).

Rozdział 6

Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z cyberbezpieczeństwem

1. Zgłoszenie incydentu jest rejestrowane przez ASI.
2. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie itp.).
3. Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent cyberbezpieczeństwa, dokonywana jest jego ocena istotności. Powyższe działania przeprowadza ASI.
4. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   a. powstałe szkody będące wynikiem incydentu;
   b. wpływ incydentu na działanie systemów;
   c. wpływ incydentu na ciągłość działania;
   d. koszty usunięcia skutków incydentu;
   e. szacowany czas naprawy skutków wywołanych incydentem;
   f. oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
5. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z cyberbezpieczeństwem ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
6. Zarządzając incydentem cyberbezpieczeństwa ASI zapewnia obsługę incydentu (czynności umożliwiające wykrywanie, rejestrowanie, analizowanie,

klasyfikowanie, priorytetzację incydentu), wyszukuje powiązania między incydentami, usuwa przyczyny ich wystąpienia oraz opracowuje wnioski wynikające z obsługi incydentu.

7. Jednostki organizacyjne we własnym zakresie podejmują działania naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
8. Podejmowane działania związane ze zgłaszanymi incydentami cyberbezpieczeństwa ASI odnotowuje w rejestrze zarządzania incydentami stanowiącym załącznik numer 2 do niniejszego regulaminu (*Załącznik 2 Rejestr zarządzania incydentami).*
9. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego ASI nie później niż w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).
10. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https://incydent.cert.pl. W przypadku braku możliwości przekazania go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. na numer telefonu +48223808274).
11. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018r (Dz.U. z 2020 r. poz. 1369 t.j ze zm.).
12. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa Burmistrz podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu mogą być powiadomione organy ścigania.

Załączniki:

Załącznik 1 Lista potencjalnych zagrożeń.
Załącznik 2 Rejestr zarządzania incydentami.

BURMISTRZ
mgr inż. Henryk Łapiński

Zagrożenie		Podatność	Opis zagrożenia
1.Działania celowe	**1.1 Oprogramowanie złośliwe**	a) Instalacja szkodliwego oprogramowania / działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery). *Najczęściej instalowane są poprzez otwarcie „zainfekowanego" załącznika z maila lub poprzez kliknięcie na zarażoną stronę. Maile takie zachęcają do otwarcia załącznika lub kliknięcia na hiperlink (mail z fakturą do opłacenia, mail z DHL o przesyłce, mail z rzekomym pismem urzędowym). W efekcie możemy zarazić nasz komputer lub wiele komputerów w sieci* *Działające szkodliwe oprogramowanie może wywołać różnorodne skutki:* • Przejęcie konta pocztowego do wysyłki spamu • Użycie przejętych komputerów do kopania kryptowalut • Użycie przejętych komputerów do ataków DOS • Użycie przejętych komputerów do śledzenia haseł użytkowników celem uzyskania dostępu do systemów i plików • Użycie przejętych komputerów do uzyskania pełnego dostępu do wewnętrznej sieci i kopiowania danych i baz danych (kradzież) *Szkodliwe oprogramowanie:* *Wirusy i trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.* *Backdoory - Instalują się z maili lub z hiperlinków w mailach. Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza.* *Keyloggery - Programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi.* *Exploity / exploitpaki - Oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.*
	1.2 Przełamanie zabezpieczeń	a)Phishing, cybersquatting (podrabianie stron)	• Mail z prośbą o zalogowanie się (pod pretekstem weryfikacji danych lub informowanie o próbie włamania na konto) do „podróbki" strony, np. bankowej, lub pseudo konta gmail i w rezultacie przejęcie hasła. • Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www. Zamiast logować się do www.mbank.pl logowanie byłoby w www.rnbank.pl

		b) Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (brute force) : • do baz danych • do serwera • do aplikacji www (np. do wordpressa) • do poczty • do windows na stacjach roboczych • do routera • do firewalla
		c) Ataki na oprogramowanie - Włamania z wykorzystaniem luk typu zero day	Zero-day to błędy w oprogramowaniu, do których autor nie przygotował jeszcze poprawek / aktualizacji. Informacje o nich są sprzedawane i wykorzystywane przez intruzów.
		d) Ataki na oprogramowanie - Włamania z wykorzystaniem najczęstszych błędów programistycznych	*Programiści pisząc programowanie często popełniają te same, znane błędy.* *Przykładowo: możliwość wpisania ujemnej liczby sztuk w formularzu zamówienia, możliwość odgadnięcia numeru zamówienia innego klienta i wpisanie go w pasku adresu przeglądarki w celu wyświetlenia szczegółów.*
		e) Włamania z wykorzystaniem API (interfejsów programistycznych)	*Niektóre aplikacje pozwalają na zdalne zarządzanie nimi przez specjalnie zaprojektowane funkcje/usługi sieciowe. Np. baza danych może pozwalać na podłączenie się do niej administratorowi w celu wykonania prac naprawczych lub backupu. Dostęp ten odbywa się przy użyciu domyślnych loginów i haseł, co stanowi zagrożenie.*
		f) Ataki na oprogramowanie - Namierzanie wersji testowych (np. strona www)	*Niektóre aplikacje posiadają swoje kopie utrzymywane do celów testowych. Są one często gorzej zabezpieczone i łatwiej jest się do nich włamać, a mogą zawierać również krytyczne dane ze środowiska produkcyjnego. Przykładem może być kopia serwera wykonana w celu przetestowania nowej wersji aplikacji. Często udaje się je namierzyć wpisując np. zamiast adresu www.strona.pl adres test.strona.pl .*
		g) Włamanie do sieci poprzez WIFI	Uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do sieci bezprzewodowej
		h) Włamanie z sieci zewnętrznej do sieci wewnętrznej	Włamania z zewnątrz poprzez nieodpowiednio zabezpieczone i skonfigurowane punkty styku z Internetem oraz udostępnione w Internecie serwery i aplikacje.

		i)Nieuprawniony dostęp do sieci z użyciem hakerskiego urządzenia	Możliwość wpięcia hakerskiego urządzenia do łatwo dostępnych urządzeń sieciowych wewnątrzorganizacyjnych, celem uzyskania dostępu do sieci przez to urządzenie z zewnątrz. Możliwość uruchomienia tzw. wrogiego access pointa w celu przechwycenia klientów sieci bezprzewodowej. Zagrożenie dla nast. elementów: • gniazdka sieciowe w korytarzach, w sali konferencyjnej • skanery, drukarki na korytarzach • switche w miejscach dostępnych
		j)Atak ransomeware	*Ransomeware - Program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny zainfekowanej strony. Są też znane przypadki infekcji poprzez sieć lokalną. Odszyfrowanie wymaga zapłaty np. 500 USD. Bardzo groźny*
		k) Ataki MAN-IN-THE-MIDDLE	Zmuszenie komputerów w sieci lokalnej do komunikowania się za pośrednictwem komputera intruza. Umożliwia przechwytywanie i podsłuchiwanie ruchu w sieci.
		l) Eskalacja uprawnień	• Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych • Przejęcie uprawnień użytkownika zaawansowanego • Przejęcie uprawnień administratora • Przejęcie uprawnień systemowych • Przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji)
		m) Atak DOS / DDOS	Atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania. Atak dotyczy głownie stron i aplikacji www. Np. wypełnienie i wysłanie kilka milionów razy formularza kontaktowego (za pomocą skryptu) i spowodowanie zapełnienia dysku. *Zmasowany atak pojedynczego atakującego (DOS) lub z wielu komputerów jednocześnie (DDOS) na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować"*
		n) Nieuprawniony dostęp lub włamanie do pomieszczeń	Dostęp do: • Budynków • Pomieszczeń biurowych • Archiwów • Serwerowni • Miejsc przechowywania kopii bezpieczeństwa Może skutkować: • dostępem do danych w wersji papierowej • dostępem do plików lub aplikacji lub baz danych • zainstalowaniem nieautoryzowanych urządzeń do dostępu do sieci wewnętrznej • kradzieżą komputerów, nośników

		o) Nieuprawniony dostęp do infrastruktury IT oraz do programów	• brak kontroli nad dostępem do serwera, plików, programów, komputerów • nadane zbyt wysokie uprawnienia użytkownikom • dostęp osób nieupoważnionych do kopii bezpieczeństwa • łatwy dostęp osób nieupoważnionych do danych prezentowanych na monitorach, drukarkach, kserokopiarkach • niezabezpieczona praca zdalna użytkowników lub serwisu IT
	1.3 Publikacje w sieci internet	a) Pomawianie, treści obraźliwie	• przejęcie strony www, BIP
	1.4 Gromadzenie informacji	a)Podsłuch	• podsłuch danych przesłanych drogą mailową • podsłuch danych podczas korzystania z aplikacji webowych • podsłuch podczas korzystania z formularzy kontaktowych • podsłuch podczas zdalnego dostępu do sieci wewnętrznej przez Internet
		b) Skanowanie sieci i usług	*Udostępniane w Internecie serwery, urządzenia sieciowe i aplikacje oraz serwisy www mogą być namierzane przez intruzów poprzez skanowanie adresów IP. Polega to na próbach łączenia się z wszystkimi znanymi usługami w celu sprawdzenia, które z nich są dostępne w naszej sieci i w jakiej wersji. Dzięki temu możliwe jest znalezienie usług nieaktualnych i zawierających błędy.*
	1.5 Czynnik ludzki	a)Nakłanianie do wykonania czynności	• Mail z dyspozycją przelewu wysłany do księgowej z rzekomego konta „Prezesa" • Fax/mail z fakturą od rzekomego „dostawcy" z informacją o zmianie numeru konta bankowego do opłacenia faktur
		b) Podrzucone nośniki danych	Atakujący pozostawia w biurze lub w dziale księgowości specjalnie przygotowany pendrive z zainstalowanym samo uruchamiającym się szkodliwym programem. W wielu przypadkach z CIEKAWOŚCI pracownicy sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery).
		c) Ataki telefoniczne	• Intruz podający się za „naszego informatyka" prosi o podanie hasła pod pretekstem sprawdzania lub naprawy naszego systemu informatycznego • Intruz przedstawia się jako „serwisant Orange lub Netii" naprawiający usterkę i prosi o wejście na określoną stronę internetową w ramach testowania łącza internetowego • Intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację" lub prosi o udostępnienie pulpitu
		d) Udostępnianie danych osobom nieupoważnionym z sieci publicznej (przez internet)	• dostęp do danych osobowych poprzez stronę www bez logowania się • dostęp do danych osobowych poprzez stronę www po zalogowaniu się (użytkownik może przeglądać dane osobowe innych użytkowników) • dostęp do katalogów udostępnionych pod publicznym adresem IP plików z danymi osobowymi lub kopii bezpieczeństwa (bez logowania się) • udostępnianie plików zaindeksowanych przez roboty google na skutek braku komend chroniących katalogi webowe przez taką indeksacją • przesłanie lub wydawanie informacji osobie nieupoważnionej

2 Działania niecelowe	**2.1 Wypadki i zdarzenia losowe**	a)Kradzież / zagubienie sprzętu i nośników poza organizacją	Kradzież / zagubienie: • laptopów • smartfonów, • pendrive • dysków wymiennych
		b) Awarie / uszkodzenia elementów IT	Awarie: • dysków • stacji roboczych • urządzeń sieciowych/routerów • drukarek / skanerów • serwera
		c) Błąd / awaria oprogramowania	Awarie: • programu kadrowo-płacowego • poczty • aplikacji www (np. do wordpressa) • bazy danych
		d) Pożar / eksplozja	• Pożar obiektu • Pożar serwerowni • Pożar serwera • Zniszczenie serwerowni (np. wybuch gazów technicznych)
		e) Zalanie	• Zalanie serwerowni • Zalanie archiwum (powódź, zalanie z rur)
		f) Przegrzanie / zbyt duża wilgotność	• wysoka temperatura w serwerowni • wysoka wilgotność w archiwum
		g) Awaria zasilania	• skoki napięcia • przerwy w dostawie zasilania
		h) Awaria łączy telekomunikacyjnych	Krytyczne dla administratora świadczącego usługi wymagające „internetu", usługi chmurowe, ISP oraz dostawcy platform SaaS
	2.2 Czynnik ludzki	a)Łatwo dostępne, łatwe lub standardowe hasła	• Ujawnianie haseł • Nieprawidłowe przechowywanie (karteczki, pliki) • Stosowanie domyślnych haseł producenta • Stosowanie słownikowych lub popularnych haseł, np. Grazynka1, qwerty, 12345678 • Stosowanie jednego hasła do wielu (często wszystkich) systemów

		b) Ataki na sprzęt - Włamania do urządzeń nieaktualizowanych	Ataki na urządzenia sieciowe oraz inne, które działają dzięki umieszczonemu na nich oprogramowaniu (firmware) Zagrożenie dla nast. elementów: • routery • switche • access pointy • firewall • macierz • dysk NAS *Brak aktualizacji tego oprogramowania (firmware) skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy.*
		c) Ataki na sprzęt - Włamania do urządzeń nieodpowiednio skonfigurowanych	Ataki na błędnie skonfigurowany sprzęt lub sprzęt działający z ustawieniami fabrycznymi. Zagrożenie dla nast. elementów: • routery • switche • access pointy • firewalle • macierze • dyski NAS *Błędy konfiguracyjne popełniane przez administratorów mogą ułatwiać hackerom włamanie się do sieci lub urządzenia.Powodem jest najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia.Przykładem jest np. pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej routera z poziomu Internetu.*
		d) Ataki na sprzęt - Włamania z użyciem niezabezpieczonych interfejsów lokalnych	Atakujący wpina się do urządzeń IT przez ich niezabezpieczone porty konfiguracyjne (USB, Ethernet lub COM - szeregowe) Zagrożenie dla nast. elementów: • routery • switche • firewalle • macierze • serwery *Administratorzy często pozostawiają te porty niezabezpieczone, co powoduje ryzyko wpięcia się do powyższych urządzeń i ich skonfigurowania przez hakera.*

		e) Ataki na sprzęt - Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze)	Atakujący wykorzystuje do włamania usługi sieciowe, których działanie w danym środowisku nie jest wymagane Zagrożenie dla nast. Usług: • DHCP • DNS • SSH • http • telnet • FTP • SMTP • SNMP *Urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy.*
		f) Ataki na oprogramowanie - Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu	Atak z wykorzystaniem znanych dziur w niezaktualizowanym oprogramowaniu Zagrożenie dla programów • Systemy operacyjne na stacjach roboczych • Systemy serwerowe • Przeglądarki www • Wordpress, Drupal • Dedykowany CMS • Adobe • Flash • Java • (podaj inne aplikacje niewymienione) *Istniejące błędy oprogramowania pozwalające na przełamanie zabezpieczeń są upubliczniane po tym, jak producent oprogramowania przygotuje odpowiednią łatę lub aktualizację. Jeżeli nie zainstalujemy tych aktualizacji, narażamy się na atak, np. zdalny dostęp do systemu lub wykonanie złośliwego kodu (instalacja backdoora, exploita, ransomeware)*
		g) Nieuprawniona modyfikacja / usunięcie	• niezamierzone lub pomyłkowe zmodyfikowanie / usunięcie danych • sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji
		h) Nieuprawnione kopiowanie danych	• kopiowanie danych z katalogów, dysków, baz, programów • kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą
		i)Brak / błędy w wykonywaniu kopii bezpieczeństwa	• doraźne lub za rzadkie wykonywanie kopii • błędy podczas procesu wykonywania kopi • niemożność odtworzenia kopii ze względu na zmiany w oprogramowaniu

		j) Nieprawidłowe / brak procedur niszczenia nośników z danymi –	• wyrzucenie uszkodzonych nośników bez ich zniszczenia • wyrzucanie dokumentów papierowych na śmietnik lub pozostawienie dokumentów w miejscu publicznym • wyrzucenie niezniszczonych , HD, pendrive, DVD
		k) Nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	• naprawa sprzętu z nośnikami bez umowy lub bez standardu bezpiecznej naprawy
		Nieprzestrzeganie procedur	• świadome naruszenie pisemnych lub ustnych procedur np. niewylogowywanie się z systemu, przekazywanie haseł osobom nieupoważnionym, naruszenie polityki czystego ekranu lub czystego biurka • naruszenia powyżej wskazane na skutek braków w inteligencji lub z powodów niewiedzy
		l) Pomyłki i błędy administratorów, użytkowników	• udostępnienia katalogów i dysków, serwerów ftp, aplikacji z danymi do powszechnego dostępu przez sieć publiczną –z powodu „ułatwienia pracy" administratorów systemów • łatwe logowanie się do baz i programów „login admin, hasło admin1" • dostęp do programów testowych (z prawdziwymi danymi osobowymi) bez logowania • pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia
		m) Błędy projektowe / konfiguracyjne	• błędy programistów prowadzące do udostępniania danych z tworzonych lub administrowanych programów • niezabezpieczenie danych w katalogach i bazach webowych i przed indeksacją robotów google
		n) Brak aktualnej dokumentacji (instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania)	• Brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania • Brak instrukcji instalacyjnych i konfiguracyjnych środowiska lub oprogramowania *Zagrożenie związane z możliwymi trudnościami w odtworzeniu środowiska i zarządzania nim, gdy np. odejdzie pracownik IT lub będzie on niedostępny podczas krytycznej awarii*
		o) Nieprawidłowe / brak umowy o współpracy	Nieprecyzyjnie określone odpowiedzialności we współpracy, co stwarza ryzyko braku zabezpieczeń
		p) Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	*Należy uwzględnić, że umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy*
		r) Upadek firmy outsourcingowej lub dostawczej	• brak zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji • Utrata usługi / aplikacji, którą świadczy pomiot przetwarzający

BURMISTRZ

mgr inż. Henryk Łapiński

Załącznik 2 Rejestr zarządzania incydentami

LP.	Data i czas zgłoszenia	Zgłaszający	Zdarzenie / Incydent (opis)	Czy zgłoszono do CSIRT NASK	Systemy / komponenty kórych dotyczył incydent	Skutki / zmiany	Podjęte działania	Uwagi, wnioski
1								
2								
3								
4								
5								
6								
7								

BURMISTRZ
mgr inż. Henryk Łapiński

Prowadzący rejestr: *(ASI)*