SZKOLENIE OPERATORA GAZOCIĄGÓW PRZESYŁOWYCH GAZ-SYSTEM S.A.

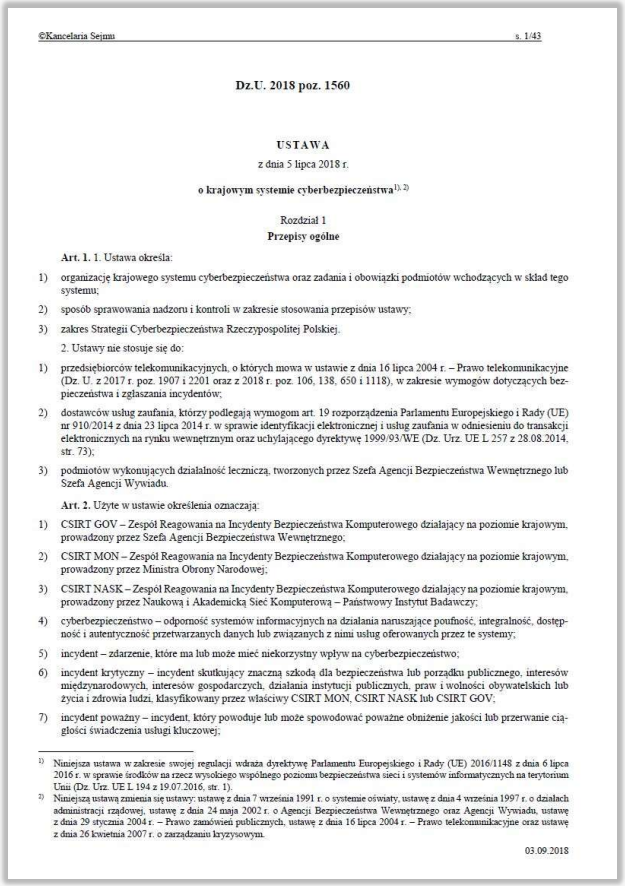
Zagrożenia cyberbezpieczeństwa oraz dobre praktyki zabezpieczenia się przed cyber-zagrożeniami

GAZ-SYSTEM CERT
Telefon alarmowy:
+48 22 220 11 11
e-mail: **cert@gaz-system.pl**

Wersja 4.0 z dnia 01.02.2024

PODSTAWY PRAWNE

Działając zgodnie z **Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa**, Operator Gazociągów Przesyłowych GAZ-SYSTEM.S.A., jako **operator usługi kluczowej** zobowiązany jest do zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.



Dz.U. 2018 poz. 1560

USTAWA

z dnia 5 lipca 2018 r.

o krajowym systemie cyberbezpieczeństwa[1), 2)]

Rozdział 1
Przepisy ogólne

Art. 1. 1. Ustawa określa:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

2. Ustawy nie stosuje się do:

1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138, 650 i 1118), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;
2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73);
3) podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

Art. 2. Użyte w ustawie określenia oznaczają:

1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
2) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;
3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
4) cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
6) 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;
7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;

---

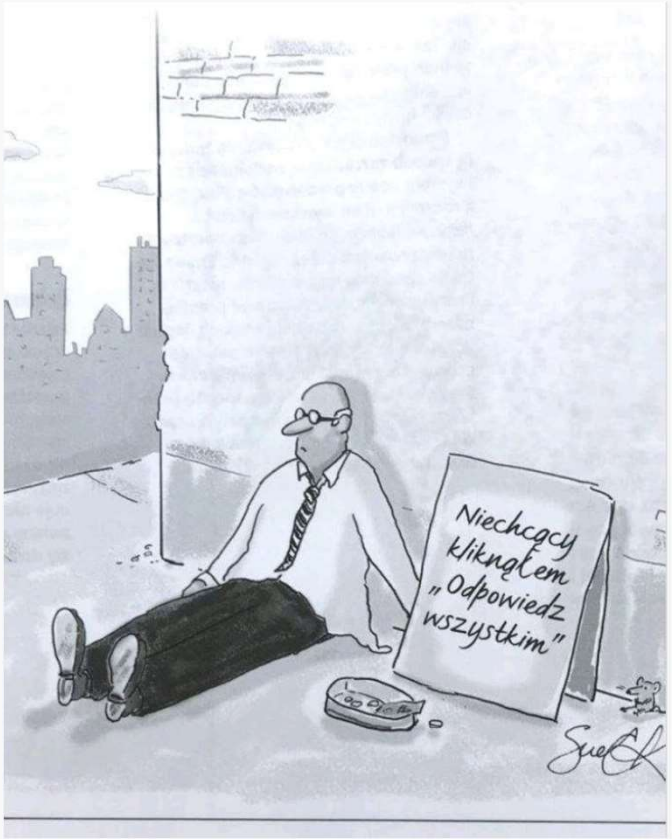
1) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1).
2) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 7 września 1991 r. o systemie oświaty, ustawę z dnia 4 września 1997 r. o działach administracji rządowej, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

03.09.2018

PODSTAWOWE ZAGROŻENIA TELEINFORMATYCZNE

PODSTAWOWE ZAGROŻENIA TELEINFORMATYCZNE

- **Wyciek informacji** (w formie elektronicznej lub fizycznej).
- **Ataki typu (D)DoS** - odmowa usługi, realizowana poprzez odpowiednio generowany ruch sieciowy, który „paraliżuje" różne funkcjonalności atakowanych urządzeń.
- **Malware** - uciążliwy lub szkodliwy typ oprogramowania, który ma na celu potajemnie uzyskać dostęp do urządzenia bez wiedzy użytkownika w celu zainfekowania lub wykradzenia danych (wirusy, konie trojańskie, robaki, **ransomware**).
- **Phishing** - metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań.
- **Socjotechnika** - zespół technik służących osiągnięciu określonych celów poprzez manipulację.



Źródło: www.pinterest.com

ISTOTNE ZAGROŻENIA TELEINFORMATYCZNE

[1] Metody manipulacji człowiekiem
[2] Wyłudzanie informacji poufnych lub nakłanianie do określonych działań przez podszywanie się pod jakąś osobę / instytucję
[3] (Rozproszona) odmowa usługi, ang. (Distributed) Denial of Service

GAZ system

INCYDENT/ZDARZENIA NOSZĄCE ZNAMIONA INCYDENTU

INŻYNIERIA SOCJOTECHNICZNA

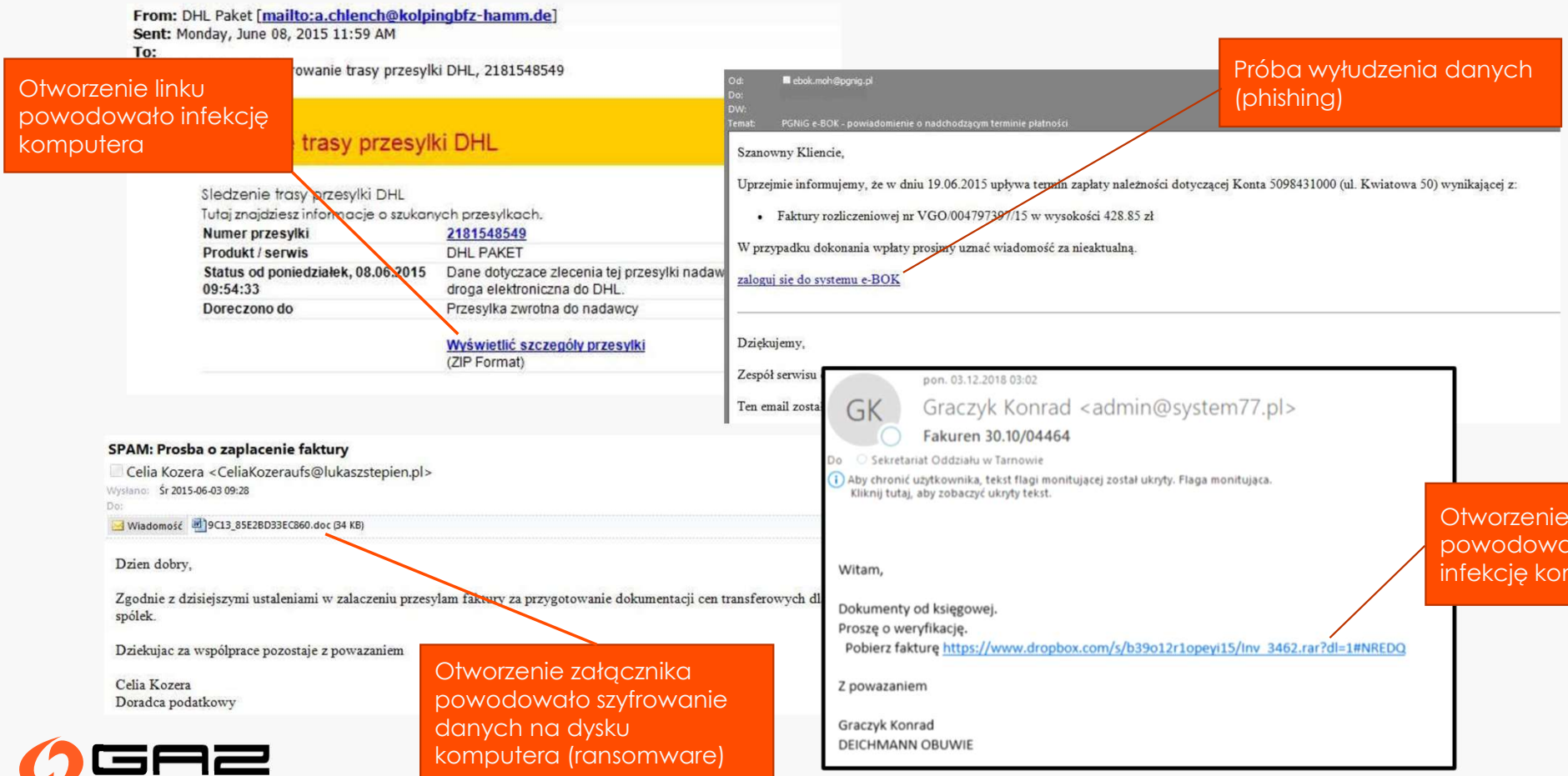
Loginy i hasła bywają bardzo często pozyskiwane **metodami inżynierii socjotechnicznej poprzez podszywanie się** atakującego pod „zaufane" osoby / podmioty / firmy współpracujące i nakłanianie pracowników atakowanej organizacji do wykonania określonej akcji lub przekazania określonej informacji. W efekcie prowadzi to najczęściej do utraty poufności ważnych danych (np. poświadczeń użytkownika do systemu) stanowiąc istotny element w całym w łańcuchu cyberataku. **Ataki prowadzone są drogą elektroniczną, przez SMS i komunikatory społecznościowe (smshing), rozmowy telefoniczne (vishing) lub osobiście.**

W przypadku użytkowania systemów infrastruktury krytycznej użytkownicy mogą się spodziewać ataków bardziej ukierunkowanych na konkretne osoby, **tzw. spear-phishing** czy **whaling**, gdzie atakujący posiadają już pewną wiedzę nt. swojej ofiary.

Niestety również **bardziej bezpośrednie metody** jak np.. **osobista** rozmowa z pracownikiem organizacji w charakterystycznym stroju dla tej organizacji, z przepustką wiernie naśladującą oryginał lub charakterystycznym atrybutem, często przynosi skutek. Z tego powodu wiele organizacji przeprowadza w tajemnicy przed pracownikami tego typu ćwiczenia w celu poprawy procedur i szkoleń dla pracowników.

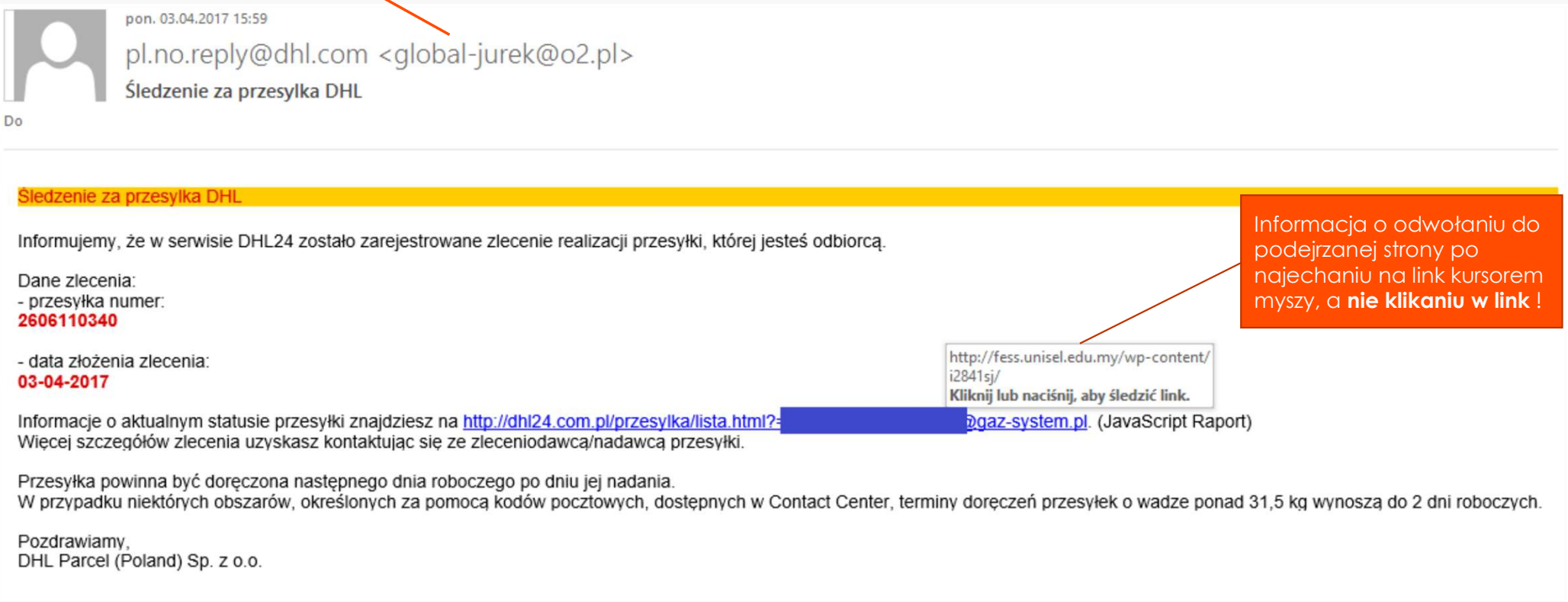
- https://www.expressvpn.com/
- https://medium.com/@Mailfence/

PRZYKŁADY FAŁSZYWYCH E-MAILI



FAŁSZYWE E-MAILE

Podejrzany adres nadawcy



pon. 03.04.2017 15:59

pl.no.reply@dhl.com <global-jurek@o2.pl>

Śledzenie za przesylka DHL

Do

Śledzenie za przesylka DHL

Informujemy, że w serwisie DHL24 zostało zarejestrowane zlecenie realizacji przesyłki, której jesteś odbiorcą.

Dane zlecenia:
- przesyłka numer:
2606110340

- data złożenia zlecenia:
03-04-2017

http://fess.unisel.edu.my/wp-content/i2841sj/
Kliknij lub naciśnij, aby śledzić link.

Informacje o aktualnym statusie przesyłki znajdziesz na http://dhl24.com.pl/przesylka/lista.html?[redacted]@gaz-system.pl. (JavaScript Raport)
Więcej szczegółów zlecenia uzyskasz kontaktując się ze zleceniodawcą/nadawcą przesyłki.

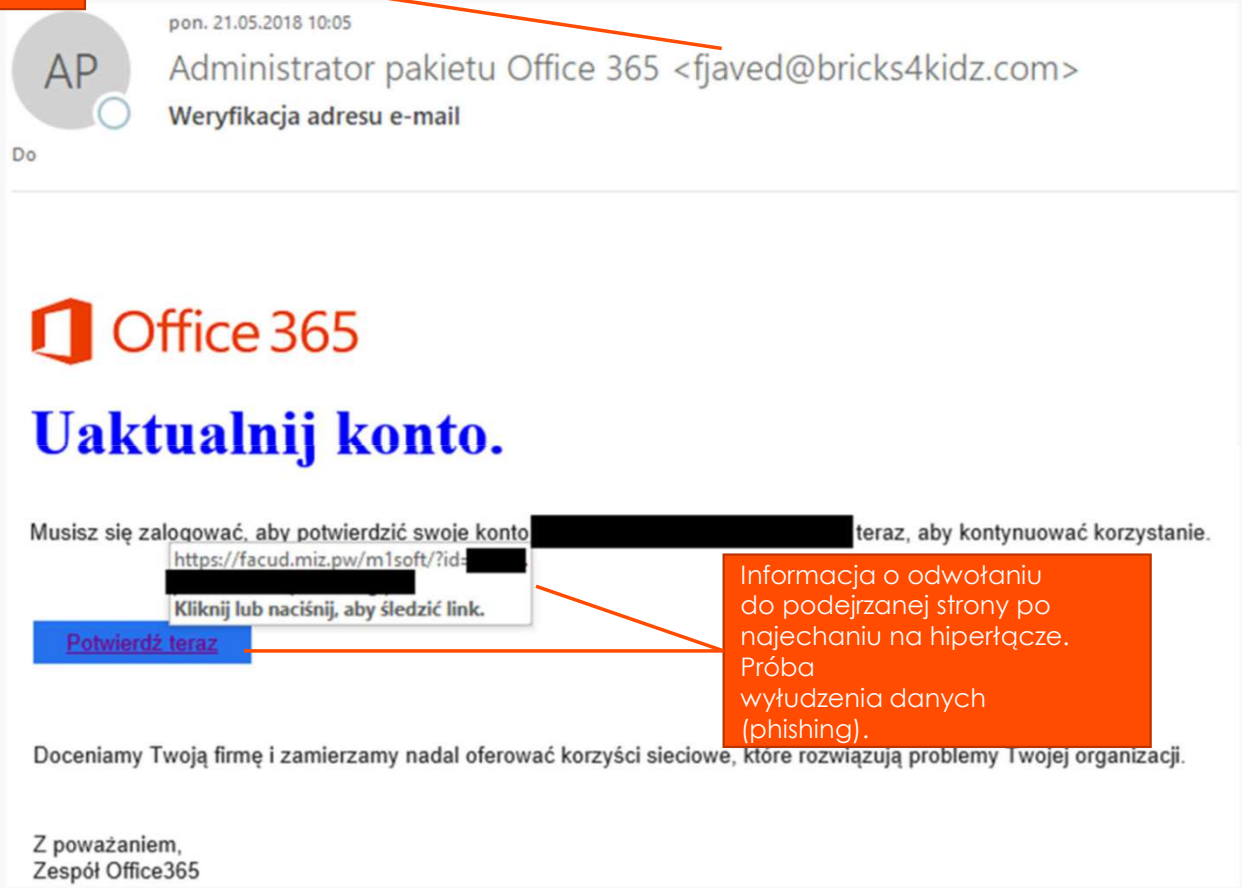
Przesyłka powinna być doręczona następnego dnia roboczego po dniu jej nadania.
W przypadku niektórych obszarów, określonych za pomocą kodów pocztowych, dostępnych w Contact Center, terminy doręczeń przesyłek o wadze ponad 31,5 kg wynoszą do 2 dni roboczych.

Pozdrawiamy,
DHL Parcel (Poland) Sp. z o.o.

Informacja o odwołaniu do podejrzanej strony po najechaniu na link kursorem myszy, a **nie klikaniu w link** !

FAŁSZYWE E-MAILE

Podejrzany adres nadawcy



pon. 21.05.2018 10:05

AP Administrator pakietu Office 365 <fjaved@bricks4kidz.com>

Weryfikacja adresu e-mail

Do

Office 365

Uaktualnij konto.

Musisz się zalogować, aby potwierdzić swoje konto [redacted] teraz, aby kontynuować korzystanie.

https://facud.miz.pw/m1soft/?id=[redacted]

Kliknij lub naciśnij, aby śledzić link.

Potwierdź teraz

Informacja o odwołaniu do podejrzanej strony po najechaniu na hiperłącze. Próba wyłudzenia danych (phishing).

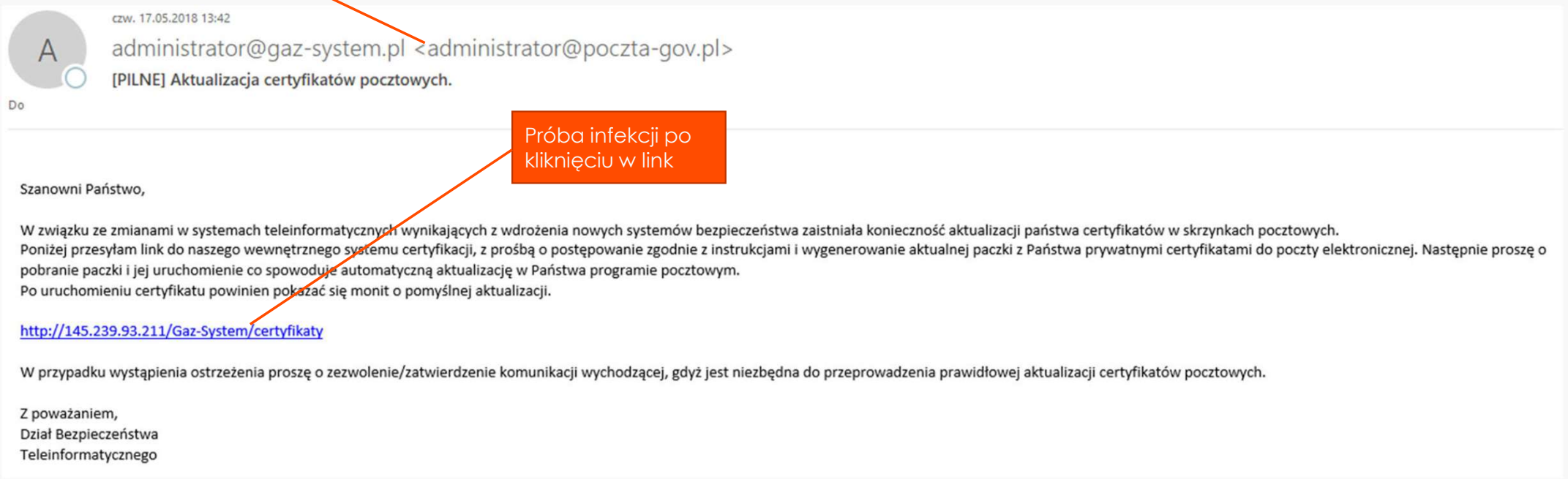
Doceniamy Twoją firmę i zamierzamy nadal oferować korzyści sieciowe, które rozwiązują problemy Twojej organizacji.

Z poważaniem,
Zespół Office365

FAŁSZYWE E-MAILE

Podejrzany adres nadawcy

Próba infekcji po kliknięciu w link



czw. 17.05.2018 13:42

A

administrator@gaz-system.pl <administrator@poczta-gov.pl>

[PILNE] Aktualizacja certyfikatów pocztowych.

Do

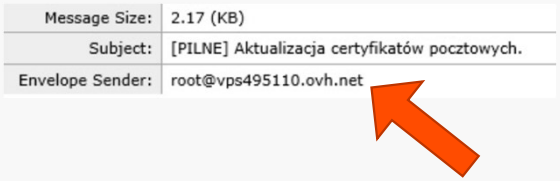
Szanowni Państwo,

W związku ze zmianami w systemach teleinformatycznych wynikających z wdrożenia nowych systemów bezpieczeństwa zaistniała konieczność aktualizacji państwa certyfikatów w skrzynkach pocztowych.
Poniżej przesyłam link do naszego wewnętrznego systemu certyfikacji, z prośbą o postępowanie zgodnie z instrukcjami i wygenerowanie aktualnej paczki z Państwa prywatnymi certyfikatami do poczty elektronicznej. Następnie proszę o pobranie paczki i jej uruchomienie co spowoduje automatyczną aktualizację w Państwa programie pocztowym.
Po uruchomieniu certyfikatu powinien pokazać się monit o pomyślnej aktualizacji.

http://145.239.93.211/Gaz-System/certyfikaty

W przypadku wystąpienia ostrzeżenia proszę o zezwolenie/zatwierdzenie komunikacji wychodzącej, gdyż jest niezbędna do przeprowadzenia prawidłowej aktualizacji certyfikatów pocztowych.

Z poważaniem,
Dział Bezpieczeństwa
Teleinformatycznego



Message Size:	2.17 (KB)
Subject:	[PILNE] Aktualizacja certyfikatów pocztowych.
Envelope Sender:	root@vps495110.ovh.net

FAŁSZYWE E-MAILE

Podejrzany adres nadawcy

Informacja o odwołaniu do podejrzanej strony po zeskanowaniu kodu QR. Próba wyłudzenia danych (phishing).

Od: PUESC Polska <refundacja@puesc-pl.eu>
Data: 4 kwietnia 2023
Dw: PUESC Polska <refundacja@puesc-pl.eu>
Temat: Potwierdzenie zatwierdzonego wniosku o zwrot podatku za okres od stycznia 2023 do marca 2023

Drogi Obywatelu,

Mamy zaszczyt poinformować, że Pański wniosek o automatyczny zwrot podatku za okres od stycznia 2023 do marca 2023 został pomyślnie zatwierdzony.

Aby odebrać zwrot podatku, proszę odwiedzić najbliższe biuro administracji podatkowej i przedstawić swoje dane identyfikacyjne lub zalogować się na nasz portal internetowy poprzez skanowanie poniższego kodu QR:

Prosimy o użycie tymczasowego hasła 6 [redacted] 9 podczas logowania.

Zwracamy uwagę, że tymczasowe hasło wygaśnie 24 godziny po otrzymaniu tej wiadomości, jako środek ostrożności mający na celu zapewnienie bezpieczeństwa transakcji.

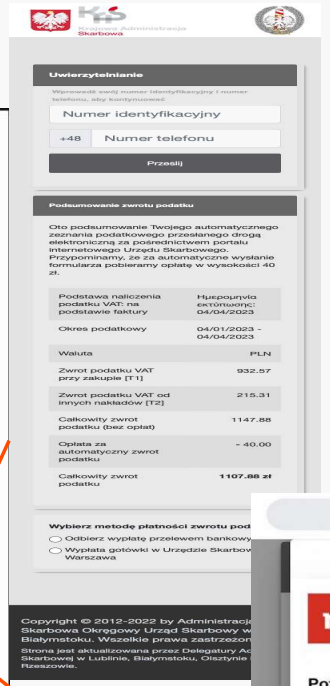
Jeśli mają Państwo jakieś dodatkowe pytania lub potrzebują pomocy, prosimy o kontakt z nami.

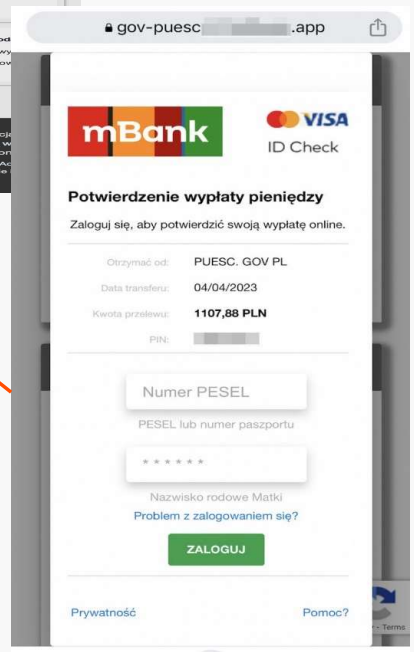
Z poważaniem,
PUESC Polska

Zeskanowanie kodu telefonem przekieruje do **fałszywej aplikacji**. Wypełnienie poleceń spowoduje przekierowanie do prawdziwego panelu płatności, gdzie wybranie swojego bank spowoduje pobieranie kolejnych danych (w tym przykładzie: nr PESEL/paszportu i nazwisko panieńskie matki), dzięki czemu przestępcy uzyskują dostęp do środków finansowych ofiary.

Linki, hiperłącza wraz z kodami/hasłami nie mogą być dystrybuowane tym samym kanałem

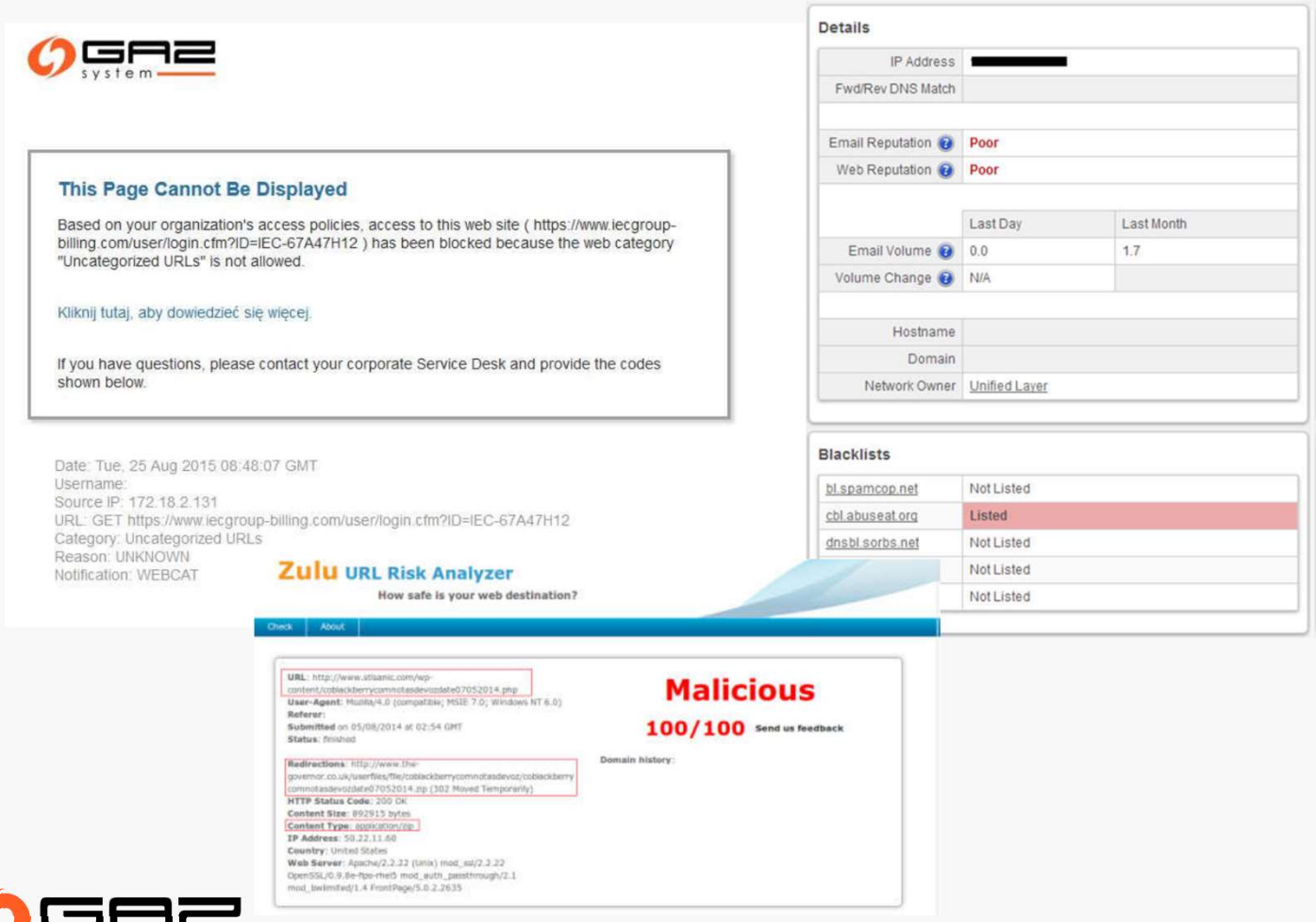
Słynny trik - presja czasu !





GAZ system

REPUTACJA STRON INTERNETOWYCH



Każda strona internetowa ma swoją reputację. Należy zachować szczególną ostrożność klikając w linki, pobierając różnorodne pliki, czy udostępniając swoje dane, szczególnie osobowe (jak np. imię i nazwisko, adres, numer telefonu, dane kart kredytowych/debetowych). Warto dokonać weryfikacji, czy dana witryna jest bezpieczna.

RODZAJE KONT

Użytkowanie każdego współczesnego systemu teleinformatycznego przeznaczonego dla wielu użytkowników wiąże się zazwyczaj z **posiadaniem w nim konta**. Konto to obiekt (zbiór danych), który opisuje użytkownika w systemie. W zależności od typu systemu najczęściej **zawiera takie atrybuty** jak: login, nazwa użytkownika, hasło, przynależność do grup, dostęp do plików i folderów.

Dla użytkowników każdego systemu bardzo ważna jest świadomość **jakie uprawnienia ma jego konto i jakie są związane z tym ryzyka**. Podwyższone uprawnienia konta (np. **konto administratora**) wiążą się z rozszerzonymi możliwościami jego wykorzystania (oprócz zakresu standardowego konta), np.:

- ✓ tworzenie, zmiana i usuwanie kont użytkowników,
- ✓ zmiany w konfiguracji systemu,
- ✓ dostęp do wszystkich plików na komputerze,
- ✓ instalacja sprzętu i oprogramowania, itp.

Im bardziej uprzywilejowane jest konto (wyższe uprawnienia), tym większe jest ryzyko jego użytkowania z punktu widzenia cyberbezpieczeństwa. Warto pamiętać, że tego typu konta są szczególnie interesujące dla atakujących.

*https://www.pymnts.com/news/security-and-risk/2019/

WYZWANIA W ZARZĄDZANIU KONTAMI

Sprawne i „bezpieczne” zarządzanie użytkownikami i hasłami jest sporym wyzwaniem.

Składa się na to wiele czynników, m.in. :

- Spora część urządzeń nie jest zarządzana przez żaden scentralizowany system do zarządzania kontami i politykami bezpieczeństwa (np. Active Directory). Co gorsza, niektóre przestarzałe komponenty nie oferują żadnej możliwości tworzenia konta i ich zabezpieczania.
- Ze względu na ograniczone zasoby występuje problem z rozdzielnością obowiązków służbowych (ta sama osoba może być głównym użytkownikiem i administratorem systemu).
- Ze względu na brak priorytetyzacji bezpieczeństwa występują „historyczne” zaniedbania, które trudno uregulować, np. ze względu na brak możliwości współpracy z odpowiedzialnym za wdrożenie rozwiązania dostawcą. Dotyczy to m.in. tzw. kont „testowych”, używania kont administratorskich przy możliwości normalnej pracy na koncie o niższych uprawnieniach, ukrytych haseł w kodzie aplikacji.
- Wprowadzanie zmian najczęściej możliwe jest tylko przy zatrzymaniu fizycznego obiektu i zawsze powstaje ryzyko pojawienia się problemów przy rozruchu instalacji po zmianach.

WYZWANIA W ZARZĄDZANIU KONTAMI

- Zakres dostępu powinien być **minimalny, ale zarazem wystarczający** do pełnienia wyznaczonych obowiązków (ang. **least privilege**). Zmiana zakresu uprawnień powinna być odzwierciedleniem zmiany zakresu obowiązków. Dzięki temu przechwycenie przez atakującego np. najczęściej używanych w systemie poświadczeń użytkownika nie oznacza od razu pełnej kontroli nad systemem.
- **Konta użytkowników Systemów powinny być implementowane w taki sposób, aby dostęp do zasobów był ograniczony tylko dla wymaganych danych na określony czas.** Stosowaną praktyką bezpieczeństwa jest ograniczanie z góry dostępu użytkowania tylko do określonej funkcjonalności przez zadany czas (np. przez określoną liczbę godzin). Po tym czasie następuje automatyczne wylogowanie użytkownika. Zasadę tą bardzo często obserwuje się dla zdalnego dostępu do systemów (np. przez tunel VPN).
- **Każdy użytkownik powinien posiadać indywidualne konto i hasło do logowania do komputerów. Użytkownicy powinni się logować tylko na czas wykonywania pracy. Użytkownicy nie mogą udostępniać swoich kont innym osobom**. Tam gdzie jest to wykonalne i uzasadnione biznesowo zawsze dąży się do implementowania indywidualnych kont. Zapewnia to możliwość śledzenia wykonywanych akcji przez poszczególnych użytkowników i przede wszystkim rozliczalność prowadzonych operacji.
- **Użytkownik konta indywidualnego powinien wylogować się po zakończeniu swojej pracy** (jeżeli nie jest to realizowane automatycznie przez system) nawet, gdy użytkownik przejmujący jego pracę ma tą samą rolę i będzie wykonywał tą samą pracę. Natomiast dość powszechnym problemem wykrywanym podczas audytów bezpieczeństwa jest problem zapisywania indywidualnych poświadczeń do systemów i trzymanie ich w miejscach dostępnych dla innych osób (np. w pokoju, do którego dostęp mają inni pracownicy organizacji, ale czasem również osoby trzecie).
- **Tworzenie i przeglądanie list dostępowych zawierające wykaz osób posiadających dostęp do Systemu wraz z określeniem poziomu uprawnień. Listy powinny być przeglądane i weryfikowane nie rzadziej niż raz na 1 rok oraz przy zmianach personalnych.** Działania te mają na celu usunięcie wszelkich nieużywanych lub nadmiarowych kont, które w wyniku luk lub przeoczeń w procesie zarządzania kontami mogą istnieć bez uzasadnienia biznesowego generując niepotrzebne ryzyko (np. istnienie konta użytkownika zwolnionego z organizacji, istnienie konta administratora dla osoby, która zmieniła rolę w organizacji). Okresowe przeglądy kont są szczególnie istotne dla kont administratorskich.

UŻYTKOWNICY SYSTEMÓW, A PRZYCZYNY INCYDENTÓW

- Najsłabszym ogniwem bezpieczeństwa organizacji są jego **pracownicy.**
- Ofiary cyberataków ufają własnym umiejętnościom ochrony danych i informacji osobowych przed potencjalnymi atakami
- Do najczęstszych błędów popełnianych przez pracowników należą:
  - **Trywialne hasła;**
  - **Odpowiadanie na maile phishingowe;**
  - Użycie **tych samych** haseł do większości kont;
  - **Dzielenie się hasłem** z innymi osobami;
  - **Zapisanie** hasła w pliku **na komputerze/ telefonie;**
  - **Niedostateczna kontrola** i monitorowanie **kont administratorów;**
  - **Omijanie procedur** szyfrowania danych.

ZASADY PRZECHOWYWANIA HASEŁ

Hasła powinny być wprowadzane przez użytkownika przy każdym logowaniu i nie mogą być zapamiętywane w Systemie w celu automatycznego logowania. Zapamiętywanie poświadczeń na maszynie, na której są wprowadzane, niepotrzebnie rozszerza płaszczyznę możliwych ataków.

Hasło tworzymy sami, przechowujemy w głowie, nie piszemy na kartkach, nie przyklejamy do monitora, pod klawiaturę itp. Ujawnienie hasła jest incydentem bezpieczeństwa.

Istnieje możliwość generowania i przechowywania haseł w aplikacjach zwanych Menadżerami Haseł np. KeePass.

KeePass Password Safe

https://www.enisa.europa.eu
https://keepass.info/

NAJPOPULARNIEJSZE HASŁA

TOP 10 2020	TOP 10 2021	TOP 10 2022	TOP 10 2023
1. 123456	1. 123456	1. **password**	1. 123456
2. 123456789	2. 123456789	2. 123456	2. 123456789
3. picture1	3. 12345	3. 123456789	3. qwerty
4. 111111	4. qwerty	4. guest	4. password
5. 12345678	5. password	5. qwerty	5. 12345
6. 1234567	6. 12345678	6. 12345678	6. qwerty123
7. abc123	7. 111111	7. 111111	7. 1q2w3e
8. senha	8. 123123	8. 12345	8. 12345678
9. qqww1122	9. 1234567890	9. **col123456**	9. 111111
10. password	10. 1234567	10. 123123	10. 1234567890

Takich haseł nie należy stosować. Hasła typowo słownikowe są bardzo łatwe do złamania !!!

https://cybernews.com/best-password-managers/most-common-passwords/

JAK BUDOWAĆ SILNE HASŁA

`Galwaniczny123$`
`zaq1@WSXcde3$RFV`
`admin.1admin.1admin.1admin.1`

`WlazlKostekNaMostekIStuka`
`zielonyParkingDla3malychSamolotow`
`DwaBialeLatajaceSophisticatedKroliki`

- Silne hasła można budować używając pełnych zdań
- Należy unikać cytatów bez znaczących modyfikacji
- Hasło powinno składać się z przynajmniej pięciu słów

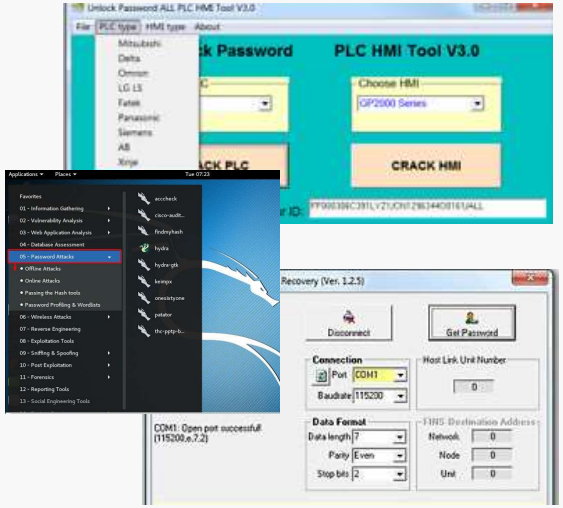
GAZ system

https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

PRZYKŁADOWE ZAGROŻENIA

Niestety proste zabezpieczenia do systemów mogą być w wielu przypadkach łamane przy użyciu **znanych od lat metod ataków i ogólnie dostępnych narzędzi**. Istnieje **wiele gotowych dystrybucji systemów operacyjnych z wbudowanymi bazami narzędzi przeznaczonymi do łamania haseł**. Poniżej wymieniono przykładowe metody stosowane do takich ataków :

- **Atak siłowy (ang. Brute Force Attack) -** atak polegający na łamaniu poświadczeń użytkowników przez **sprawdzanie różnych możliwych kombinacji** liter, cyfr, znaków (często z ustawieniem złożoności haseł, aby przyspieszyć proces). Pomimo, że metoda jest dość prymitywna, ciągle bywa skuteczna, przeważnie w przypadku krótkich haseł.
- **Atak słownikowy (ang. Dictionary Attack) -** zbliżony do ataku „brute force", jednak nie sprawdza każdej kombinacji znaków, a **testuje wszystkie hasła z wgranego słownika**. Słowniki te są tworzone m.in. na podstawie haseł, które wyciekły do internetu w wyniku cyberataków. Stosuję się także maski i kombinacje wyrazów. Istotne jest, że jeśli hasło nie jest zawarte w załadowanym słowniku narzędzia to nie zostanie złamane tą metodą. Warto pamiętać, że obie metody **mogą być realizowane w trybie online lub offline** (jeżeli przechwycono np. zaszyfrowane hasło).
- **Key Logger -** rodzaj oprogramowania/ sprzętu, który **rejestruje bez wiedzy użytkownika znaki wprowadzane** z klawiatury do systemu zainfekowanego urządzenia. Bardziej rozbudowane programy monitorujące aktywność użytkownika potrafią także przychwytywać zrzuty ekranów, logi z systemu i aplikacji, dźwięk z mikrofonu i wysyłać przechwycone dane za pośrednictwem poczty elektronicznej lub serwera FTP w postaci szyfrowanej.



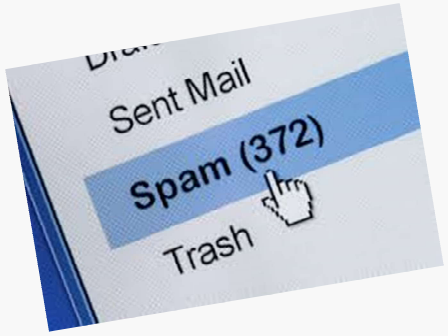
Zrzuty ekranów z przykładowych programów do łamania haseł.*

* https://www.opentechinfo.com/

KONTO POCZTOWE...

Nie należy wykorzystywać służbowego adresu e-mail do celów prywatnych i odwrotnie!!!

Bazy danych adresów e-mailowych są sprzedawane lub wykradane, a potem wykorzystywane podczas różnego rodzaju ataków, czego efektem jest otrzymywanie na skrzynkę e-mail spamu, zainfekowanych wiadomości czy phishingu. **Nie wykorzystuj służbowego adresu e-mail do newslettetrów/subskrypcji czy zakładania kont na portalach internetowych, jeżeli nie jest to związane z zakresem Twoich obowiązków.**



https://www.prnewswire.com/
https://www.techrepublic.com
https://www.komputerswiat.pl/

Odchodząc od komputera pamiętaj o jego zablokowaniu

Po zakończeniu pracy komputer powinien być wyłączony

Sprzętu służbowego, jak np. laptopy czy telefony nie należy zostawiać bez opieki

https://www.enisa.europa.eu

Korzystając ze sprzętu służbowego pamiętaj o bezpieczeństwie przetwarzanych danych

Pracując poza siecią firmową warto korzystać z VPN i sieci internetowej udostępnionej za pomocą karty SIM/modem czy hot spot z telefonu;
Nie zaleca się korzystania z ogólnodostępnych/darmowych sieci Wi-Fi

https://www.enisa.europa.eu

RODZAJE URZĄDZEŃ WYMIENNYCH ORAZ MOBILNYCH

Urządzenia wymienne i mobilne pomimo swojej popularności stanowią często **niedoceniany przez użytkowników (a czasem i administratorów) potencjalny wektor ataków**.

Mówiąc o **urządzeniach wymiennych** mamy na myśli m.in. :

- ✓ Pamięci USB, karty SD, MMC, SIM,
- ✓ Płyty CD, DVD,
- ✓ Zewnętrzne dyski twarde,

Do **mobilnych urządzeń** zaliczamy z kolei m.in. :

- ✓ Telefony komórkowe / smartfony, PDA,
- ✓ Tablety, czytniki e-booków (np. Kindle),
- ✓ Laptopy (niniejszy materiał nie skupia się na tych urządzeniach).

Urządzenia wymienne w przypadku stosowania w niekontrolowany sposób mogą **m.in. łatwo wprowadzać złośliwe oprogramowanie do środowiska IT** wykorzystując luki techniczne urządzeń i systemów komputerowych oraz luki proceduralne w organizacji. Dobrym przykładem jest **brak ograniczania użycia portów USB** na stacjach komputerowych.

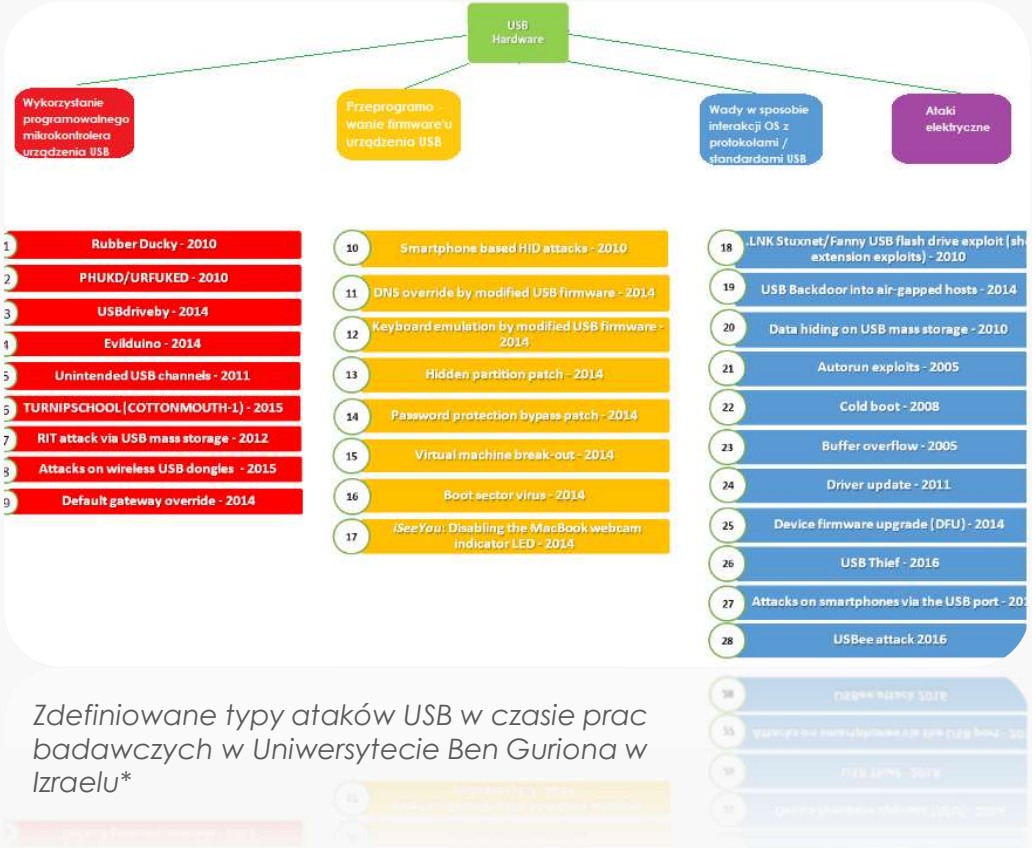
Innym spotykanym jest używanie urządzeń mobilnych **jako hot-spotów dla stacji komputerowych,** np. w razie potrzeby sporadycznej aktualizacji lub co gorsza **na potrzeby nie związane z zadaniami służbowymi**

https://deepsatech.com/
https://learningclassesonline.blogspot.com/2018/03/what-are-computer-storage-devices-and.html

NOŚNIKI USB I ZWIĄZANE ZAGROŻENIA

Naukowcy z Uniwersytetu Ben Guriona w Izraelu opracowali listę **29 różnych typów ataków związanych z nośnikami USB** i podzielili je na **4 kategorie**:

- **wykorzystanie wad w sposobie normalnej interakcji systemów operacyjnych z protokołami / standardami USB**,
- **przeprogramowanie firmware'u urządzenia USB w celu wykonywania szkodliwych działań** (takich jak pobieranie złośliwego oprogramowania, kradzież danych itp.),
- **atak z wykorzystaniem programowalnego mikrokontrolera urządzenia USB** (np. urządzenie wygląda z zewnątrz dokładnie jak inne tego samego typu, ale zachowuje się jak zupełnie inne urządzenie i wykonuje określone zadania),
- **ataki elektryczne**, które trwale niszczą sprzęt, gdy podłączane urządzenie USB wyzwala szybki cykl ładowania / rozładowania.



*Zdefiniowane typy ataków USB w czasie prac badawczych w Uniwersytecie Ben Guriona w Izraelu**

* https://www.bleepingcomputer.com

NOŚNIKI USB I ZWIĄZANE ZAGROŻENIA

Przenośne nośniki pamięci USB są również **skutecznie wykorzystywane w atakach socjotechnicznych**, co ma swoje odzwierciedlenie w historii cyberataków, ale było także udowadniane różnymi testami. W jednym z tego typu testów przeprowadzonych w USA rozrzucono 5 typów zainfekowanych dysków USB na parkingach campusu uniwersytetu* w celu zebrania statystyk odnośnie korzystania przez ludzi z urządzeń o nieznanym pochodzeniu.

W rezultacie :

- **48%** rozrzuconych nośników zostało **zabranych i podłączonych do komputera** oraz został **uruchomiony co najmniej jeden plik**.
- Z 5 grup nośników najczęściej podłączono urządzenia, do których były **przypięte klucze lub miały etykietkę Confidential**…
- Pierwsze podłączenie do komputera nastąpiło **już w ciągu 6 minut od pozostawienia nośnika na parking**…

Rodzaje nośników pamięci użyte w czasie badań inżynierii socjotechnicznej

* University of Illinois Urbana-Champaign campus , https://elie.net/

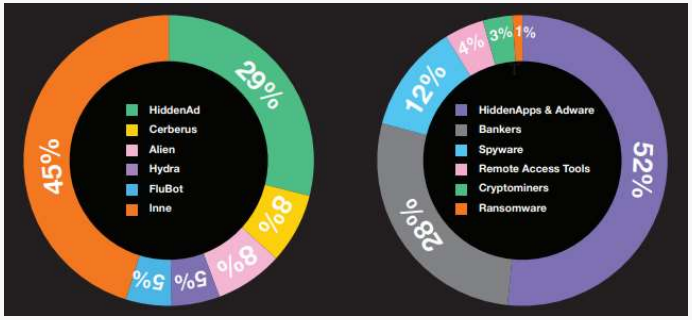
URZĄDZENIA MOBILNE I ZWIĄZANE ZAGROŻENIA

Należy mieć świadomość, że używanie urządzeń mobilnych (w szczególności smartfonów / tabletów) w celu podłączania do infrastruktury sieciowej, która obejmuje systemy, bez wyraźnego uzasadnienia biznesowego i spełnienia określonych wymagań, **generuje niepotrzebne ryzyko dla bezpieczeństwa tych systemów**. Ryzyko jest jeszcze wyższe, jeśli używane są **urządzenia prywatne,** które nie są zarządzane w żaden sposób przez organizację i nie są wymuszane na nich jakiekolwiek techniczne środki bezpieczeństwa. Najbardziej prawdopodobnymi wektorami ataku z użyciem urządzeń mobilnych wydają się: utrata poufności informacji, rekonesans systemu jako jeden z elementów łańcucha ataku oraz ataki odmowy usługi (DoS).

Ryzyko wynika m.in. z faktu, że wspomniane urządzenia mobilne (smartfony/tablety) najczęściej **nie posiadają oprogramowania antywirusowego**, **aktualizacje** systemu operacyjnego są **implementowane nieregularnie**, mogą być na nich **instalowane dowolne aplikacje**, **aplikacje nie są uruchamiane w izolowanym środowisku** (kontenerze), **urządzenia te podłączane są do różnych sieci**, najczęściej **publicznych**.

Jednocześnie w ostatnich latach daje się zaobserwować **wyraźny wzrost liczby złośliwego oprogramowania w aplikacjach mobilnych** oferowanych w „sklepach" internetowych. A niemalże każdego dnia rejestruje się ok **12 000 instancji nowego złośliwego** kodu na smartfonach. Jednak użytkowników żyje w przekonaniu, że ich urządzenia mobilne nie są możliwym celem dla złośliwego oprogramowania.

Najczęściej występujące złośliwe oprogramowanie w sieci mobilnej



Rodzaje zagrożeń w sieci mobilnej wykrywane

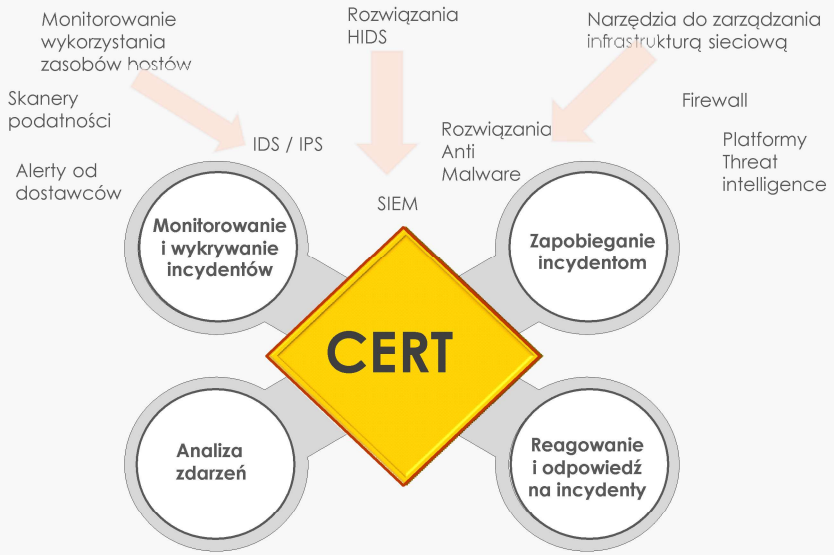
https://mks-vir.pl/download/press/Raport_Orange_2022.pdf
https://www.computerworld.pl/news/Wirusy-na-Androida-popularne-i-niebezpieczne-zagrozenia,437669.html
https://www.gdatasoftware.com/

GAZ-SYSTEM CERT

Terminem, który łączy się z aspektem incydentów bezpieczeństwa jest tzw. **CERT (ang. Computer Emergency Response Team),** czyli scentralizowana i wyspecjalizowana jednostka, która zajmuje się wykrywaniem, przyjmowaniem i reagowaniem na zdarzenia cyberbezpieczeństwa na poziomie organizacyjnym i technicznym.

Jednostka GAZ- SYSTEM CERT składa się z zespołu analityków, inżynierów i ekspertów podzielonych na 3 grupy (tzw. I, II i III linia), które mają różne zadania w zarządzaniu potencjalnymi incydentami cyberbezpieczeństwa.

W nagłych wypadkach lub w sytuacjach kryzysowych prosimy o kontakt z GAZ-SYSTEM CERT, wysyłając wiadomość na wskazany e-mail: cert@gaz-system.pl , lub dzwoniąc pod numer telefonu alarmowego: +48 22 220 11 11



ZGŁASZANIE INCYDENTÓW PRZEZ PODWYKONAWCÓW I PRACOWNIKÓW STRON TRZECICH

Podwykonawcy i pracownicy stron trzecich są zobligowani do zgłaszania zdarzeń i incydentów bezpieczeństwa oraz zaobserwowanych lub podejrzewanych podatności cybernetycznych. Zgłoszenia należy kierować do koordynatora prac po stronie Spółki.

Budowanie świadomości wśród pracowników firm zewnętrznych, **nt. znaczenia ich postawy i ich możliwego wpływu** na działanie Spółki jest jednym z kluczowych elementów budowania sprawnie działającego mechanizmu wykrywania i zarządzania incydentami.

Niektóre etapy cyberataków nie są wykrywane przez narzędzia / oprogramowanie przez długi czas lub są wykrywane, ale informacja nie jest nigdzie przekazywana w czasie rzeczywistym. Natomiast **pewne symptomy naruszeń** infrastruktury **mogą być zauważone przez użytkownika systemu jako odchylenia od normalnego działania.**

Przykładem może być samoczynny restart / zawieszenie się stacji komputerowej lub aplikacji bez żadnego powiadomienia, zmodyfikowana funkcjonalność systemu, itp..

Dlatego też nie wolno bagatelizować takich sytuacji i przyjmować biernej postawy.

Podwykonawcy i pracownicy stron trzecich są zobligowani do niewykorzystywania zauważonych podatności systemu. Wykorzystanie lub próba wykorzystania zauważonych podatności powinna być traktowana jako incydent bezpieczeństwa.

Niestety skala wykrywanych podatności jest duża i wyraźne widać trend wzrostowy w porównaniu z poprzednimi latami.

Dlatego zauważone podatności systemów należy **niezwłocznie zgłaszać** do koordynatorów umów **bez podejmowania jakichkolwiek prób samodzielnego ich sprawdzenia** (np. w celach samodzielnej oceny lub celach edukacyjnych) ze względu **na ryzyko naruszenia** dostępności / poufności integralności informacji.

GAZ system

* Mandiant's M-Trends report, 2017 r.

ZABEZPIECZANIE DOWODÓW

Po zgłoszeniu zdarzenia lub incydentu cyberbezpieczeństwa wymagane jest niezwłoczne zabezpieczenie dowodów

Proces gromadzenia informacji nt. zdarzeń / incydentów oraz ich zabezpieczania musi być prowadzony tak, **aby nie utraciły one atrybutów dostępności, integralności i poufności - materiały te muszą zachowywać wartość dowodową.** Przykłady dowodów, które mogą być wykorzystywane w dalszej analizie incydentu to **:** zainfekowane nośniki danych, logi zapory ogniowej, systemu IDS, systemu operacyjnego lub aplikacji z danego komputera, itp.

Aby informacje zachowały wartość dowodową, niezmiernie istotny jest sposób postępowania z nimi:

- ✓ nośniki danych zabezpiecza się w miejscu o ograniczonym dostępie, rejestruje się kto i kiedy miał do nich dostęp,
- ✓ zapisywane jest pochodzenie zabezpieczonych materiałów,
- ✓ nie wolno dopuść do zniszczenia lub utraty nośnika,
- ✓ absolutnie w żaden sposób nie modyfikuje się danych istniejących na oryginalnym nośniku / źródle,
- ✓ użytkownicy systemów nie powinni podejmować samodzielnych prób szukania innych źródeł danych lub odzyskiwania utraconych danych (ryzyko zmanipulowania dowodów),
- ✓ zabezpieczanie danych samodzielnie powinno umożliwiać sprawdzenie ich integralności, np. przez zastosowanie sumy kontrolnej,

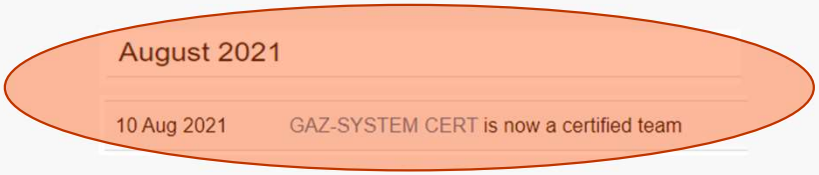
SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Od 2012 roku Spółka GAZ-SYSTEM ma wdrożony System Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO/IEC 27001. System ten stanowi zbiór skoordynowanych procesów, procedur, zasobów, sposobów organizacji, planowanych działań itp. mający na celu zapewnienie skutecznego zarządzania bezpieczeństwem informacji.

Od 2015 roku Spółka ma wdrożony System Zarządzania Ciągłością działania zgodnie z normą ISO/IEC 22301. System ten stanowi zbiór skoordynowanych procesów, procedur, zasobów, sposobów organizacji, planowanych działań itp. mający na celu zapewnienie skutecznego zarządzania ciągłością działania.

Źródło: https://www.infratech.com.sa

CERTYFIKACJA ZESPOŁU GAZ-SYSTEM CERT DO POZIOMU „CERTIFIED”



Zespół **GAZ-SYSTEM CERT** jest certyfikowanym członkiem renomowanej międzynarodowej organizacji GEANT Trusted Introducer.

Od dnia 10 sierpnia 2021 r. GAZ-SYSTEM CERT jest zespołem z **najwyższym poziomem certyfikacji „CERTIFIED”**, który otrzymał jako szósty krajowy zespół CERT (wcześniej otrzymali: Orange, PKO BP, NASK, PSE, PGE).

Usługa Trusted Introducer Service - zwana także TI - została utworzona przez europejską społeczność CERT w 2000 r. w celu zaspokojenia potrzeb i budowy infrastruktury usługowej, zapewniającej istotne wsparcie dla wszystkich zespołów ds. bezpieczeństwa i reagowania na incydenty.

PODSUMOWANIE

- Kiedy jesteśmy **pytani o informacje, które naszym zdaniem są poufne**, **zawsze należy upewnić się**, że osoba/podmiot, która nas pyta jest do tego autoryzowana, a my możemy przekazać taką informację. Warto pamiętać, że **ponad 21% pracowników firm pada ofiarą ataków** inżynierii socjotechnicznej…
- Należy **być podejrzliwym i dociekliwym**, gdy widzisz **niecodzienne albo „dziwne" zdarzenie.** Pamiętajmy, że współczesne ataki ukierunkowane na osiągnięcie poważnego skutku w systemach infrastruktury krytycznej są coraz bardziej złożone, składają się z wielu różnych etapów i mogą trwać wiele miesięcy lub nawet dłużej.
- Jeżeli dostrzegamy **wyraźne słabości lub problemy** dotyczące kont / haseł dotykających ważne komponenty zawsze warto **upewnić się**, że ich administrator ma tego świadomość i przekazać mu taką informację.
- Przed zmianą uprawnień do systemu należy otrzymać **odpowiednie szkolenie**, które wyjaśnia **ryzyka i zasady** związane z korzystaniem z nadawanych uprawnień.
- Należy **bez zwłoki reagować i zgłaszać** zauważone incydenty cyberbezpieczeństwa. To samo należy robić w przypadku zaobserwowania podejrzanego / nietypowego zachowania się użytkowanego systemu.
- **Nie należy podejmować prób samodzielnej analizy dowodów** potencjalnego incydentu ze względu na możliwość zmanipulowania lub utraty dowodów (najczęściej nieświadomie).

PODSUMOWANIE

- **Samodzielne próby wykorzystania zauważonych podatności** (np. w celach edukacyjnych lub oceny podatności) **są traktowane jako incydenty cyberbezpieczeństwa.**
- Urządzenia wymienne posiadają wiele zalet i przyjęły się na dobre zarówno w świecie IT, jednakże ich używanie **może stanowić duże zagrożenie** dla istotnych komponentów infrastruktury.
- Używanie urządzeń wymiennych wiąże się z koniecznością **zadbania zarówno o wysoką świadomość użytkowników** dotyczącą ryzyka używania tych urządzeń, **wdrożenia procedur organizacyjnych, jak i środków technicznych.**
- **Zapisanie informacji** poufnych na urządzeniach wymiennych oraz mobilnych **implikuje również konieczność zadbania o prawidłowe i trwałe usunięcie** tych danych, co w wielu przypadkach nie jest równoznaczne z prostym kliknięciem opcji Usuń np. w systemie operacyjnym.
- Do innych ważnych zasad, które regulują korzystanie z omawianych urządzeń można zaliczyć :
  - **Uzasadnione ograniczanie** dostępu do fizycznych portów dla większości użytkowników, szczególnie gdy nie ma potrzeby ich stosowania,
  - Używanie narzędzi antywirusowych do **skanowania tych urządzeń**,
  - **Ewidencjonowanie urządzeń**, określanie ich właścicielstwa oraz **unikanie korzystania z urządzeń**, których **pochodzenie nie jest znane.**

PODSUMOWANIE

„Cyberataki to cały czas niezbadane terytorium. Będzie gorzej, nie lepiej”

„Cyberataki stanowią większe zagrożenie dla ludzkości niż broń jądrowa”

„Cyberprzestępczość jest największym zagrożeniem każdego przedsiębiorstwa na świecie”

Warren Buffett- *amerykański ekonomista, inwestor giełdowy, przedsiębiorca (powszechnie uważany za jednego z najlepszych inwestorów na świecie).*

Virginia Rometty, *amerykańska prezes i dyrektor generalny firmy informatycznej* ***IBM***

1980 2000 2010 2019 2023

Źródło: www.forbes.com Źródło: https://www.wprost.pl/tylko-u-nas/481839/czy-polska-jest-gotowa-na-cyberatak.html
Źródło: https://www.rp.pl/Telekomunikacja-i-IT/305219945-Hakerzy-i-szantazysci-zagrozeniem-dla-przetwarzajacych-dane.html

Źródło: http://www.gaz-system.pl/nasze-inwestycje/krajowy-system-przesylowy/tlocznia-gazu-gustorzyn/ ;
https://wiadomosci.wp.pl/wielka-brytania-oskarza-rosyjski-wywiad-wojskowy-o-cyberataki-6302350746838657a

PAMIĘTAJ O TYM, ŻE...

…najbardziej niebezpieczne miejsce Internetu i każdego systemu znajduje się…

…pomiędzy krzesłem a klawiaturą komputera…

Źródło: https://mitsmr.pl/cyberzarty-czyli-memy-tworzone-przez-sztuczna-inteligencje/

DZIĘKUJEMY ZA UWAGĘ