enterprise europe network

„Europejskie Przedsiębiorstwo”

Zarządzanie bezpieczeństwem informacji w działalności Małych i Średnich Przedsiębiorstw, czyli… jak skutecznie chronić nasze ważne dane

18 kwietnia 2019 r. Warszawa

PARP Grupa PFR / Centrum Rozwoju MŚP

enterprise europe network

European Commission

www.een.org.pl

Zanim zaczniemy:

- Kilka słów o …
- „Kontrakt”
- O czym mówić nie będziemy?

Zakres spotkania:

1. Prawne aspekty związane z bezpieczeństwem informacji
2. Przykłady kradzieży i wycieku danych z przedsiębiorstw
3. Świat nie kończy się na „RODO” czyli chrońmy dane osobowe, ale bez uszczerbku dla innych ważnych informacji
4. Zagrożenia przy korzystaniu z Internetu: poczta e-mail, strony www, serwisy społecznościowe
5. Czy pendrive od znajomego może być niebezpieczny? Bezpieczne korzystanie z przenośnych nośników pamięci

Zakres spotkania:

6. Etyczny hacking, czyli jak ustrzec naszą organizację przed prawdziwym atakiem
7. Jakie jest Twoje hasło do systemów? Bezpieczeństwo i zasady stosowania haseł
8. „Najsłabsze ogniwo” i „podejrzane e-maile” – przykłady ataków socjotechnicznych
9. Skuteczne metody ochrony przed phishingiem
10. Polityki bezpieczeństwa informacji firmy jako skuteczne narzędzie ochrony informacji

„Ryzyko pozostaje kwestią drugorzędną

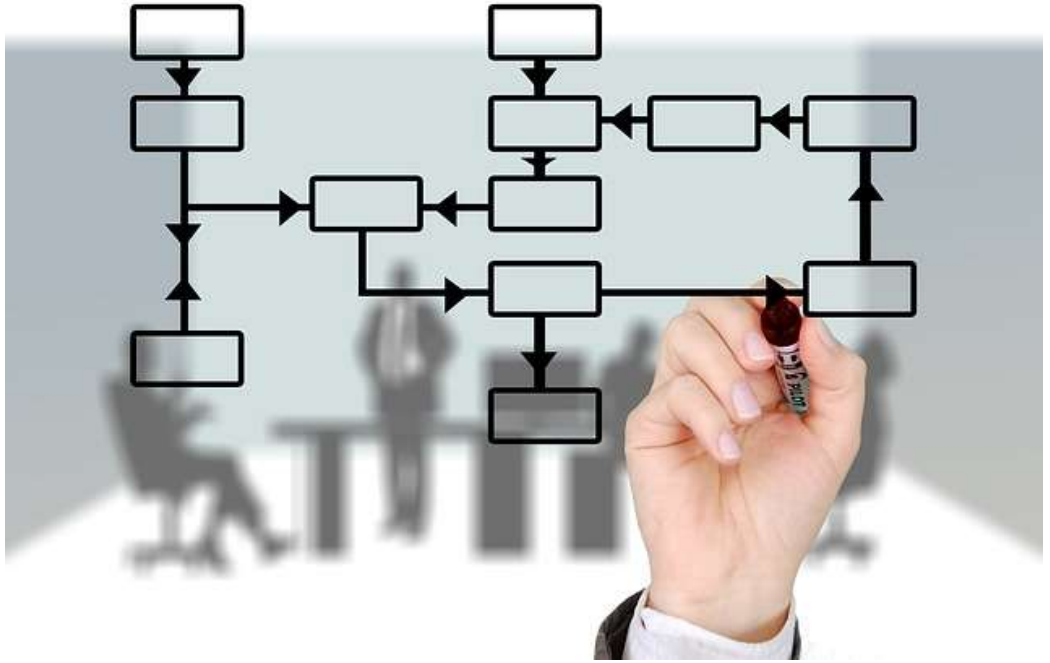
… tylko tak długo jak

długo organizacji sprzyja szczęście”

źródło: Carl. L. Pritchard „Zarządzanie ryzykiem w projektach. Teoria i praktyka”

Polityka bezpieczeństwa w organizacji

- Polityka organizacyjna
- Polityka ochrony fizycznej
- Polityka personalna
- Polityka Bezpieczeństwa Informacji



PARP Grupa PFR / Centrum Rozwoju MŚP
enterprise europe network
European Commission

Bezpieczeństwo informacji

Bezpieczeństwo informacji to:

- **poufność** przetwarzanej informacji,
- **integralność** przetwarzanej informacji
- **dostępność** do przetwarzanej informacji

… w ramach 15% informacji ze szkolenia … ☺

Bezpieczeństwo informacji w systemach IT

Bezpieczeństwo informacji w systemach IT (wymagania):

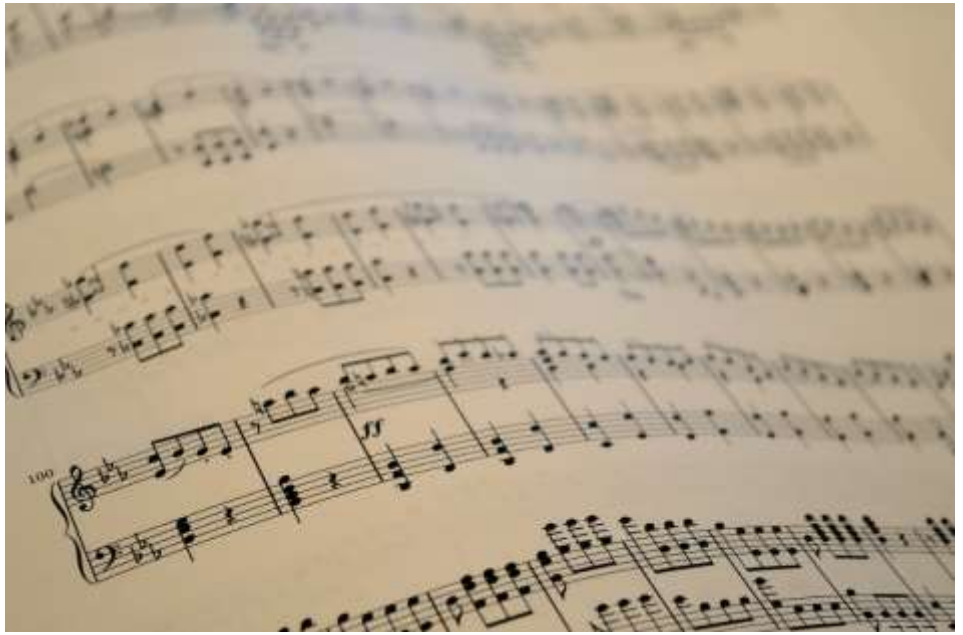
- Poufność informacji (uniemożliwienie dostępu do danych osobom trzecim).
- Integralności informacji (uniknięcie nieautoryzowanych zmian w danych).
- Dostępność informacji (zapewnienie dostępu do danych, w każdym momencie żądanym przez użytkownika)

… a w systemach IT dodatkowo:

- **Rozliczalność operacji** wykonywanych na informacjach (zapewnienie przechowywania pełnej historii dostępu do danych, wraz z informacją

Kultura ochrony informacji

- Uświadomić wartość informacji
- Proces rekrutacji
- Cyberbezpieczeństwo
- Kadra zarządzająca: "ponad prawem„?



PARP Grupa PFR
Centrum Rozwoju MŚP
enterprise europe network
European Commission

Prawne aspekty związane z bezpieczeństwem informacji

Prawna ochrona informacji

- Ochrona Danych Osobowych
- Tajemnica przedsiębiorstwa
- Tajemnice zawodowe
- Ochrona Informacji Niejawnych
- Ochrona Praw Autorskich

Przykład - Naruszenie zasad pracodawcy

Można dyscyplinarnie zwolnić:

za instalowanie pirackich programów na komputerze pracodawcy
(Sąd Rejonowy dla Warszawy Pragi-Północ - sygn. akt VI P 32/16)

lub

oglądanie pornografii - nawet jeśli zagrożenie jest tylko teoretyczne
(Sąd Rejonowy w Bełchatowie - sygn. V Pa 79/18 / V Pa 81/18),

lub

za podłączenie prywatnego pendrive'a do służbowego komputera
(wyrok Sądu Najwyższego - sygnatura akt: III PK 13/18)

Tajemnica przedsiębiorstwa

Ustawa z dnia 16 kwietnia 1993 o zwalczaniu nieuczciwej konkurencji

Przez **TAJEMNICĘ PRZEDSIĘBIORSTWA** rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności

Tajemnica przedsiębiorstwa

- Trzy warunki <u>jednocześnie:</u>
  1. informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą,
  2. jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są one powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób,
  3. uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.

Tajemnica przedsiębiorstwa (przykłady - sprzedaż)

- Lista klientów
- Poufne cenniki
- Terminy nowych umów
- Zapytania ofertowe
- Oferty

PARP Grupa PFR / Centrum Rozwoju MŚP
enterprise europe network
European Commission

Tajemnica przedsiębiorstwa (przykład - produkcja)

- Dane dotyczące dostawców
- Stosowane metody produkcji/ procedury
- Know-how
- …

PARP Grupa PFR
Centrum Rozwoju MŚP
enterprise europe network
European Commission

Tajemnica przedsiębiorstwa (przykład - finanse)

- Dokumenty finansowe
- Wynagrodzenie pracowników
- Prognozy, raporty
- Sprawozdania finansowe ?
- …

Przykłady kradzieży i wycieku danych z przedsiębiorstw


Enjoy your struggle
Because once you
succeed, you are going
to kill the story of
your success girl. Now
So, enjoy your struggle
Be single be virgin
Happy!
I Love
my
Mother

Kradzież / Wyciek danych

Kampania społeczn

Kradzież / Wyciek danych

- Media: *„Setki faktur, PIT-ów i innych dokumentów, z nazwiskami, adresami, telefonami i kwotami wypłat - … znaleźli strażnicy miejscy w jednym z kontenerów na śmieci ”*
- *Media: „Zgubiony laptop, pendrive, teczka, dysk, …”*
- *Media: „Drogowcy …”*
- *Media: „Metro zapłaciło …”*

Kradzież / Wyciek danych

- Partner biznesowy wykorzystuje nasze pomysły / rozwiązania
- Utrata bazy klientów z odchodzącym pracownikiem
- > 25% pracowników zabiera ze sobą dane


WC

Świat nie kończy się na „RODO”
czyli
chrońmy dane osobowe,
ale bez uszczerbku dla innych ważnych informacji

Prawna ochrona informacji >>> „RODO”

- **RODO -** rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (**O**gólne **R**ozporządzenie o **O**chronie **D**anych).
- **25.05.2018**
- **Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych** (Dz. U. 2018 r., poz. 1000);
- Zmiana wielu aktów prawnych

Dane osobowe

Zgodnie z art. 4 pkt 1 GDPR/RODO:

Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatorów takich jak:

- imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy,
- jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Prawna ochrona informacji >>> „RODO”

1. Prawo obywatela do bycia zapomnianym i dochodzenia roszczeń
2. Rozszerzony obowiązek informacyjny
3. Obowiązek informowania o naruszeniu ochrony danych, każdej osoby której naruszenie dotyczy
4. Przystępny język …
5. Ciągły proces a nie tylko dokumentacja
6. Dostosowanie systemów informatycznych (szyfrowanie danych, pseudonimizacja, anonimizacja)

Prawna ochrona informacji >>> „RODO”

Im mniej mam danych, tym lepiej:

1. czy mogę nie mieć?
2. od kogo?
3. po co?
4. jak długo?
5. gdzie?
6. kto ma dostęp?

Zagrożenia przy korzystaniu z Internetu

Źródła wiedzy o organizacji i pracownikach

- portale społecznościowe
- dobrzy znajomi
- sekretariat
- winda / pociąg / taksówka
- „bar”

… KRS, CEIDG …

PARP Grupa PFR / Centrum Rozwoju MŚP
enterprise europe network
European Commission

Korespondencja e-mail

- Do czego służy?
- Jak bezpiecznie przekazać załącznik?
- NIE - służbowe skrzynki do prywatnych e-maili
- NIE - prywatne skrzynki do służbowych e-maili
- e-maile do "biuro@", „kadry@", „handlowy@", "ksiegowosc@„ A co mamy zwrotnie?
- Podpisywanie cyfrowe korespondencji
- Szyfrowanie korespondencji

Korespondencja e-mail

Podstawowe **błędy** korzystania z poczty e-mail:

- Autouzupełnianie
- Błąd: DW zamiast UDW - „ukryte do wiadomości” (ang. blind carbon copy, BCC)
- Listy wysyłkowe / grupy adresatów
- Emocje …
- Prywatność w e-mail ?

Czy pendrive od znajomego może być niebezpieczny?

Urządzenia USB w firmie

- Do czego służą?
- Targi, promocja, gadżety etc.
- Przykład: „konkurs dla uczniów”
- Przykład: firma wycofuje pendrive’y
- Jak bezpiecznie korzystać? „Jak żyć?”

PARP Grupa PFR / Centrum Rozwoju MŚP
enterprise europe network
European Commission

Etyczny hacking,
czyli jak ustrzec firmę przed prawdziwym atakiem

„Ataki” … na zamówienie zarządu

Sprawdzenie podatności pracowników:

- przynęty
- interakcja
- wyspecjalizowane firmy

„Ataki” … na zamówienie zarządu

- wysłanie e-maili (sms) wyłudzających informację
- rozmowy telefoniczne
- przygotowane nośniki danych
- ustawienie fałszywych sieci Wi-Fi

- Testy podatności
- Testy penetracyjne (pentesty)
- …

Jakie jest Twoje hasło do systemów?

Jakie jest Twoje hasło do systemów?

- Hasło to **SEKRET …**

- TYLKO silne hasła, …
- Często zmieniaj hasła
- Różne hasła do różnych systemów
- Korzystaj z menedżerów haseł

PARP Grupa PFR
Centrum Rozwoju MŚP
enterprise europe network
European Commission

Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou

źródło: SplashData's Worst Passwords of 2018 / www.splashdata.com

PARP Grupa PFR / Centrum Rozwoju MŚP
enterprise europe network
European Commission

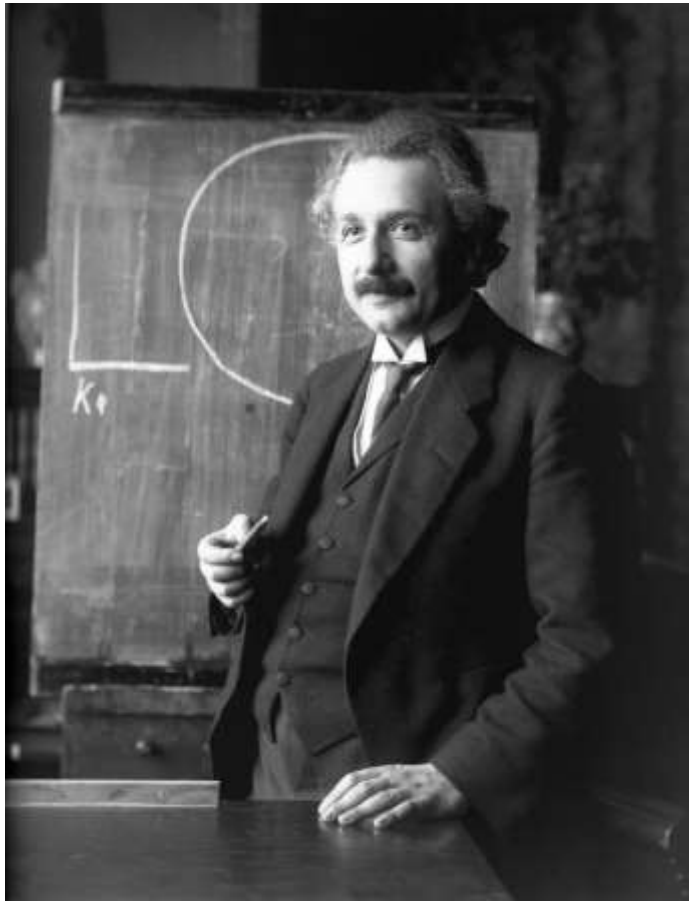
„Najsłabsze ogniwo”
i
„podejrzane” e-maile

"Tylko dwie rzeczy są nieskończone:

wszechświat i ludzka głupota, chociaż

co do pierwszego nie mam pewności„

~ Albert Einstein



Socjotechnika

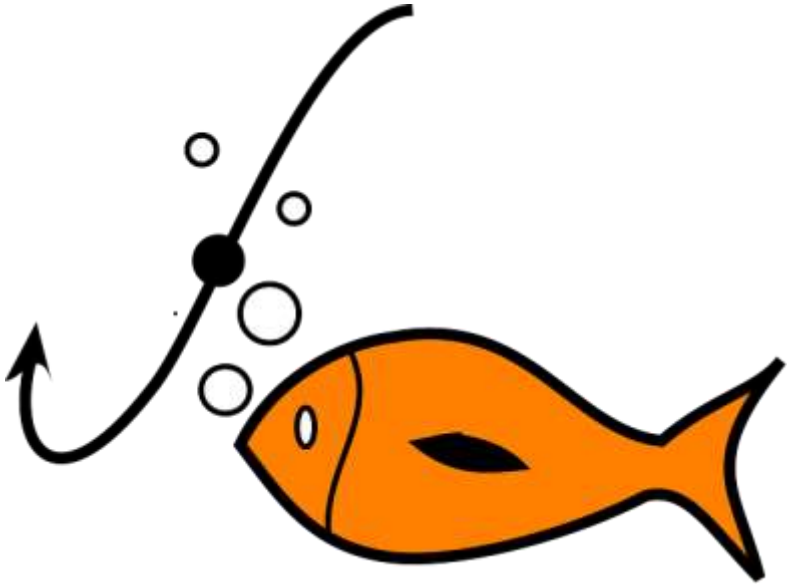
„Socjotechnika to wywieranie wpływu na ludzi i stosowanie perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości.

Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji.”

źródło: Kevin Mitnick, William L. Simon, Steve Wozniak *„Sztuka podstępu”, Wydawnictwo Helion*

Przykłady zagrożeń dla bezpieczeństwa informacji

- **PHISHING** – wyłudzanie poufnych danych: sms, e-mail, telefony



- **RANSOMWARE**
  - odszyfrowanie za okup 300 USD-1000 USD
  - milczenie za okup
  - „profesjonalna obsługa”
  - „RaaS”

NIE PŁAĆ !!!

Socjotechnika

- ✓ Założenia: wzbudzenie zaufania, poczucie winy, chęć pomocy
- ✓ Znaki ostrzegawcze: pilność, groźby, „coś dziwnego”
- ✓ Cele ataku: recepcja, kadry, księgowość

- ✓ Czynniki ułatwiające:
  - ✓ duża liczba pracowników,
  - ✓ brak systemów i zasad bezpieczeństwa
  - ✓ brak szkoleń

źródło: Kevin Mitnick, William L. Simon, Steve Wozniak *„Sztuka podstępu”, Wydawnictwo Helion*

Dziwne i ciekawe z … „naszego podwórka”

SMS:

”Witam. Na wstępie przepraszam za kłopot, ale podczas rejestracji w serwisie internetowym przez moja nieuwagę moje dziecko wpisało nieprawidłowy numer telefonu i SMS dotyczący rejestracji zamiast do nas został wysłany na Pani/Pana numer. Czy jest możliwość odesłania mi treści tego SMSa pod mój numer jeśli już dotarł lub dopiero dojdzie? Jeżeli nie sprawi to kłopotu. Będę bardzo wdzięczna za pomoc, z góry dziękuję. Anna.”

Dziwne i ciekawe z … „naszego podwórka”

- „na wnuczka” /„na policjanta” / „na chore dziecko” / „na Kuriera”
- „na pracownika banku”, „na serwisanta IT”, „na RODO”, „na cyfrowy rejestr”
- klienci banków
- fałszywe ogłoszenia o pracę
- maile z zaległą fakturą VAT
- przedsądowe wezwanie do zapłaty
- dopłaty do szkoleń z projektów UE
- …

UWAGA:

Nigdy nie otwieraj załączników i linków z e-maili oraz reklam/bannerów pochodzących od nieznanych lub podejrzanie wyglądających źródeł


67% 16:56
119119
poniedziałek, 11 marca 2019
SMS dla konta Klienta 16611346. Uplynal termin platnosci FV na kwote 25.76 zl. Prosimy o dokonanie wplaty na konto 76 1240 6960 0601 0000 1661 1346.
10:26

Odpowiedz | Odpowiedz wszystkim | Prześlij dalej

pt. 2019-04-05 03:23

ezqyrzj@ .pl <jjah@ .pl>

INFORMACJA O ZAMIARZE WSZCZECIA KONTROLI SKARBOWEJ

Do

Wiadomość | Załącznik bez tytułu 00025.txt (131 B)

_____ Antivirus _____

Zagrożenia znalezione w tej wiadomości e-mail:

dokumentacja_63579.ACE - VBS/TrojanDownloader.Agent.RBU koń trojański - usunięty
dokumentacja_63579.ACE » RAR5 » dokumentacja_63579.vbs - VBS/TrojanDownloader.Agent.RBU koń trojański - usunięty

Wersja silnika detekcji: 19144 (20190405)

wt. 2018-07-24 15:47

[redacted] Express 90983893703 <gysxxwynl@[redacted].com>

Rachunek z tytulu przechowywania przesylki, 90983893703

Szanowni Panstwo!

Staralismy sie dostarczyc twoja przesylke w czwartek, 19/07/2018. Proba doreczen
uzyskac. Aby odebrac paczke, prosimy o wydrukowanie kwitu, ktory jest dolaczon
fakturze (kwitu). Jesli przesylki nie odebrac w ciagu 48 godzin, zostanie ona zwroc

---

Numer przesylki: T90983893703
Prosimy o wplate: 862,55 pln

Pobierz faktura

śr. 2018-11-07 23:28

[redacted] Teresa <no-reply@[redacted].com>

Fakuren 1825645910/2643654222

Do [redacted]

Wiadomość | Faktura 0811076691.rar (721 B)

Dzien dobry,

W zalaczeniu zestawienie do rozliczenia kosztow.

Details here

Żegnaj!

[redacted] Teresa

GRUPA [redacted]

Glowna Ksiegowa Barbara [redacted] <barbara.[redacted]@[redacted].pl>

Potwierdzenie P³atnoœci

Do [redacted]

Wiadomość | Załącznik bez tytułu 00084.txt (131 B)

Witam, w za³aczniku przesy³am potwierdzenia p³atnoœci na Pañstwa konto.

Proszê o informacjê w jakim terminie wszystko zostanie zrealizowane.

Z powa¿aniem
[redacted]

_____ [redacted] Antivirus _____

Zagrozenia znalezione w tej wiadomosci e-mail:

POTWIERDZENIE PLATNOSCI.z - VBS/Kryptik.IX kon trojanski - usuniety
POTWIERDZENIE PLATNOSCI.z > RAR5 > pko_trans_details_20180828_130451.pdfvbs - VBS/Kryptik.IX kon trojanski - usuniety
POTWIERDZENIE PLATNOSCI.z > RAR5 > pro_forma_901849099213.pdf.vbs - VBS/Kryptik.IX kon trojanski - usuniety

śr. 2018-10-03 01:47

Tomasz [redacted] <marzena@[redacted].pl>

fakturę 181002_1945

Do [redacted]

Usunęliśmy dodatkowe podziały wiersza w tej wiadomości.

Wiadomość | faktura181002_11066.rar (1 KB)

Dzień dobry

Na dzień dzisiejszy nie odnotowaliśmy wpłaty za faktury których zestawienie przesyłam w załączeniu. Jeżeli należności zostały uregulowane proszę uznać powyższą wiadomość za nieważną. W przypadku nieuregulowania płatności w terminie 7 dni od dnia

otrzymania tej wiadomości, sprawa może zostać skierowana do windykacji.

Z poważaniem,

Tomasz [redacted]

[redacted] Sp. z o.o.

śr. 2018-04-11 22:04

ZWROT KOSZTOW PODATKI <POLSKIE.PODATKI@[redacted].com>

►►►►►► FORMULARZ ZWROTU ►►►►►►►►►

Do [redacted]

Wiadomość | DYREKCJA GENERALNA FINANSA PUBLICZNA.pdf (105 KB)

finanse.mf.gov.pl/strona-glowna

Witam,

Informujemy, że przysługuje ci zwrot pieniędzy za ostatni rachunek podatkowy.
Kliknij poniższy link:

https://
e2f0ece317fba6ca903cf6ebf4cbe484.
[redacted].com/
Kliknij, aby śledzić łącze

---

zwrot kosztów → : finanse.mf.gov.pl/strona-glowna

Dobry odbiór!

Z poważaniem,

śr. 2018-06-13 06:34

Wojciech [redacted] <wojciech.[redacted].pl>

zestawienie płatności

Do [redacted]

Wiadomość | Faktura_0975.zip (183 KB)

Dzień dobry,

w załączniku przesyłam zestawienia aktualnych Pana płatności.

Z poważaniem,
Wojciech [redacted]
Biuro [redacted]

pon. 2017-04-10 11:53

24 <artur.[redacted]@[redacted].pl>

Status przesyłki [redacted]

Do [redacted]

Status przesyłki [redacted]

Szanowny Kliencie,

Informujemy, że w serwisie [redacted] zostało zarejestrowane zlecenie realizacji przesyłki, której jesteś odbiorcą.

Podgląd aktywnych zleceń dostępny jest pod adresem: http://www.[redacted].pl/report.html&email=[redacted] (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

Niniejsza wiadomość została wygenerowana automatycznie.

Dziękujemy za skorzystanie z naszych usług i aplikacji [redacted].

[redacted] Parcel

UWAGA: Wiadomość ta została wygenerowana automatycznie. Prosimy nie odpowiadać funkcją Reply/Odpowiedz

Pn 2016-06-13 15:47

[redacted] <magda.[redacted]@[redacted].pl>

Blokada konta [redacted]

Do [redacted]

Dostęp do Twojego konta Bank [redacted] został anulowany!

W trosce o bezpieczeństwo naszych klientów zablokowaliśmy konto w systemie [redacted] internet, powodem jest nieautoryzowany dostęp do konta.
W celu odzyskania dostępu prosimy o weryfikację właściciela rachunku, logując się na:

www.[redacted]/weryfikacja

Serdecznie pozdrawiamy,
Zespół Bank[redacted] S.A.

W przypadku jakichkolwiek pytań prosimy o kontakt z Infolinia [redacted]

Ten e-mail został wygenerowany automatycznie. Prosimy na niego nie odpowiadać. Bank [redacted] z siedzibą we Wrocławiu, ul. [redacted] 50 pod numerem KRS [redacted], REGON [redacted], NIP [redacted], kapitał zakładowy i wpłacony [redacted] zł.

Wchodzisz na stronę wprowadzającą w błąd

Osoby atakujące stronę **zaloguj[redacted]site** mogą podstępem nakłonić Cię do zrobienia czegoś niebezpiecznego, np. zainstalowania oprogramowania lub ujawnienia danych osobowych (takich jak hasła, numery telefonów i dane kart kredytowych).

☑ Automatycznie przesyłaj do Google szczegółowe informacje o możliwych zagrożeniach. Polityka prywatności

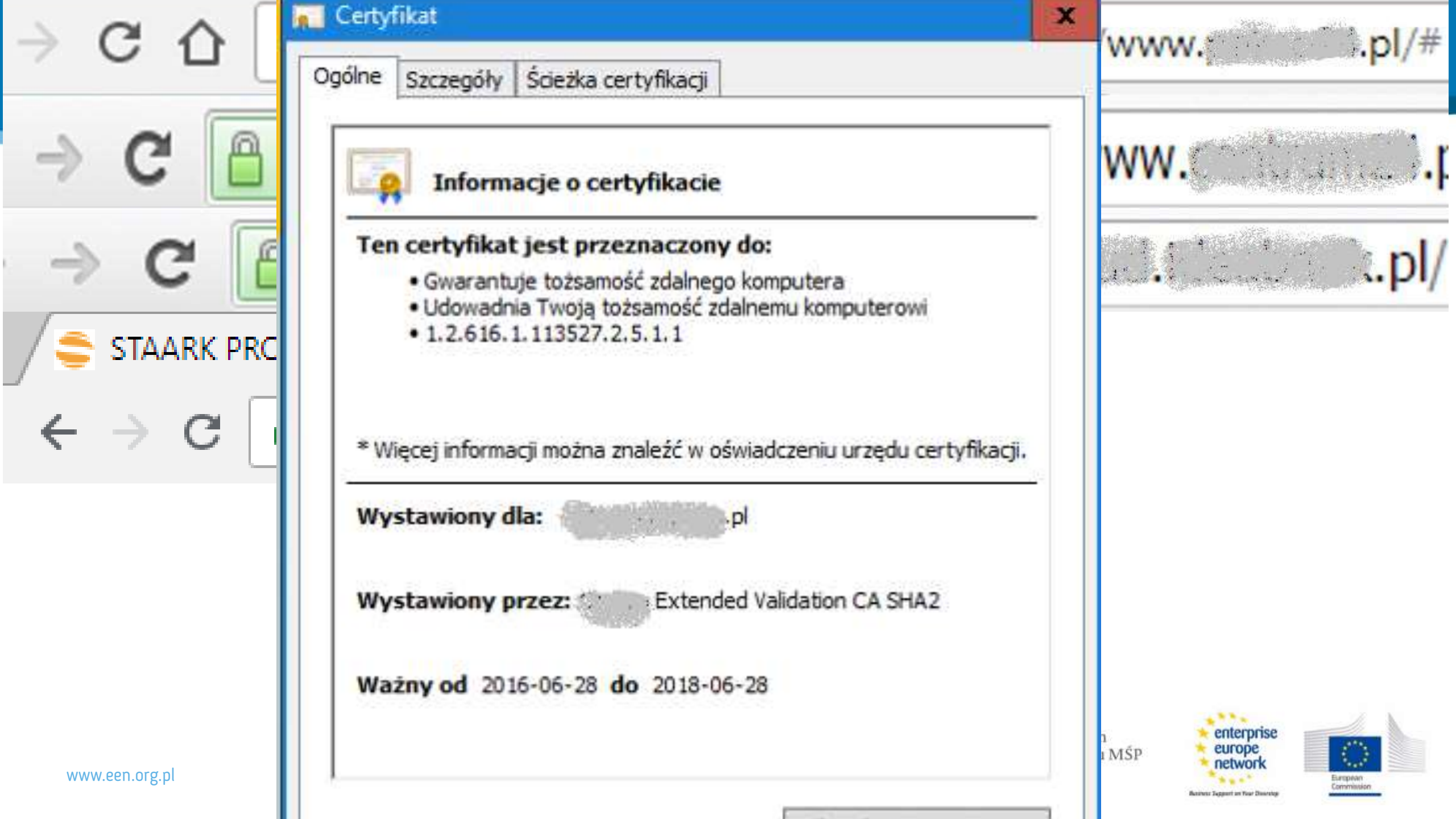
UKRYJ SZCZEGÓŁY

Powrót do bezpieczeństwa

Bezpieczne przeglądanie Google wykryło ostatnio próbę wyłudzenia informacji na stronie zaloguj[redacted]site. Strony wyłudzające informacje udają inne strony, aby Cię oszukać.

Możesz zgłosić problem z wykrywaniem lub – jeśli rozumiesz zagrożenie – wejść na tę niebezpieczną stronę.


zaloguj-
.site/?email=a


Certyfikat
Ogólne
Szczegóły
Ścieżka certyfikacji
Informacje o certyfikacie
Ten certyfikat jest przeznaczony do:
• Gwarantuje tożsamość zdalnego komputera
• Udowadnia Twoją tożsamość zdalnemu komputerowi
• 1.2.616.1.113527.2.5.1.1
* Więcej informacji można znaleźć w oświadczeniu urzędu certyfikacji.
Wystawiony dla:
.pl
Wystawiony przez:
Extended Validation CA SHA2
Ważny od 2016-06-28 do 2018-06-28
STAARK PRC
www.
.pl/#
ww.
.p
.pl/
MŚP
enterprise
europe
network
European
Commission
www.een.org.pl


https://ww

Skuteczne metody ochrony przed phishingiem

Korespondencja e-mail

Ważne pytania:

- *Nadawca?*
- *Wcześniej?*
- *Spodziewałeś się?*
- *Temat, nazwa załącznika, treść, polskie znaki?*
- *Wirusy?*

JAK SIĘ CHRONIĆ PRZED PHISHINGIEM - PODSUMOWANIE

- Otwieraj strony samodzielnie a nie przez otrzymany link
- Weryfikuj poprawność adresu e-mail nadawcy i adresów stron www
- Sprawdzaj zabezpieczenia SSL („zielona kłódka” + certyfikat)
- Oszukuj portale ☺
- Nie używaj otwartych sieci Wi-Fi
- Zainstaluj VPN na służbowych urządzeniach (dział IT pomoże ☺)
- Domeny internetowe (TLD), które warto omijać („black list”)

Wzrost świadomości !!!

Złota myśl...

„Firmy dzielą się na te co wykonują backup danych i na te co wkrótce będą go wykonywać.”

SINERSIO POLSKA SP. Z O.O.

Fot.: za zgodą Sinersio Polska Sp. z o.o.

Polityki bezpieczeństwa informacji (PBI) jako skuteczne narzędzie ochrony informacji w firmie

Polityka bezpieczeństwa informacji (PBI)

„POLITYKA BEZPIECZEŃSTWA INFORMACJI – zbiór spójnych, precyzyjnych reguł i procedur, według których firma buduje, zarządza oraz udostępnia zasoby i systemy informacyjne.”

Polityka bezpieczeństwa informacji (PBI)

- Wprowadzenie PBI chroni interesy przedsiębiorcy
- PBI pomaga wypełnić obowiązki ochrony informacji wynikające z przepisów prawa
- PBI należy dostosować do specyfiki organizacji – komunikatywność, prostota
- PBI dotyczy wszystkich systemów przetwarzania informacji: klasycznie (archiwa, kartoteki, dokumenty papierowe) jak i systemów teleinformatycznych.
- PBI - element kultury nowoczesnych organizacji

Polityka bezpieczeństwa informacji (PBI)

- ogólne zasady
- „czyste biurko i ekran”
- urządzenia mobilne
- odpowiedzialność za dane na komputerach
- korzystanie z Internetu
- korzystanie z poczty elektronicznej
- hasła dostępowe
- …

PBI - instrukcje / procedury

ZASADY OGÓLNE KORZYSTANIA ZE SPRZETU KOMPUTEROWEGO:

1) nie wolno spożywać płynów i pożywienia oraz przechowywać roślin w bezpośredniej bliskości urządzeń teleinformatycznych
2) niedopuszczalne jest korzystanie w komputerach stacjonarnych, laptopach, serwerach oraz innych urządzeniach komputerowych pracujących w systemie informatycznym organizacji z prywatnych nośników informacji

PBI - instrukcje / procedury

POLITYKA CZYSTEGO BIURKA

1) wszelkie dokumenty papierowe i nośniki komputerowe, kiedy nie są używane, przechowuje się w odpowiednich, zamykanych szafach lub innego rodzaju zabezpieczonych meblach, szczególnie poza godzinami pracy
2) w przypadku opuszczenia stanowiska pracy komputer należy zabezpieczyć przed niepowołanym dostępem innych osób poprzez zablokowanie go lub wylogowanie się

PBI - instrukcje / procedury

POLITYKA CZYSTEGO BIURKA

1) komputery nie mogą być pozostawione bez nadzoru w stanie zarejestrowania do systemów informatycznych
2) pracownicy zobowiązani są do niezwłocznego odbioru swoich wydruków z urządzeń drukujących (szczególnie dotyczy to wydruków zawierające informacje wrażliwe).

PBI - instrukcje / procedury

POCZTA ELEKTRONICZNA:

- Służbowa poczta elektroniczna jest udostępniana Pracownikom do wypełniania obowiązków służbowych.
- Wysyłanie pocztą elektroniczną wiadomości zawierających pornografię, treści dyskryminujące przedstawicieli określonej rasy, płci i religii lub dyskryminujące pod innym względem jest zakazane i może stanowić podstawę do podjęcia działań dyscyplinarnych.

PBI - instrukcje / procedury

URZĄDZENIA MOBILNE:

- Pracownicy posiadający służbowe urządzenia mobilne tj. telefony komórkowe, smartfony, tablety oraz laptopy są odpowiedzialne za używanie ich w sposób adekwatny do poziomu poufności informacji gromadzonych i przekazywanych przy ich użyciu.
- Obowiązek ochrony urządzenia mobilnego spoczywa na jego użytkowniku.

PBI - instrukcje / procedury

ZAPASOWE KOPIE DANYCH:

- Użytkownicy są odpowiedzialni za wykonywanie kopii zapasowych danych przechowywanych na swoich komputerach lokalnych.
- Do obowiązków użytkowników należy wykonywanie i przechowywanie kopii istotnych danych na dyskach sieciowych wskazanych przez Administratora lub osobę przez niego wyznaczoną.

PBI - instrukcje / procedury

HASŁA:

- Hasło do systemu musi składać się z min. 16 znaków - zawiera małe i duże litery oraz cyfry lub znaki specjalne (silne hasło)
- Zmiana hasła następuje nie rzadziej niż co 90 dni.
- Jeżeli system nie wymusza zmiany haseł użytkownik zobowiązany jest samodzielnie zmieniać hasło nie rzadziej niż co 90 dni.

PBI - instrukcje / procedury

Hasło <u>nie powinno być</u>:

- słowem ze słownika w żadnym popularnym języku,
- nazwiskiem, nazwą geograficzną, terminem technicznym lub określeniem potocznym,
- związane z życiem zawodowym lub osobistym użytkownika np. nie powinno być numerem rejestracyjnym samochodu, numerem telefonu, imieniem członka rodziny, częścią adresu, inicjałami itp.

PBI - instrukcje / procedury

Hasło <u>nie powinno być:</u>

- sekwencją kolejnych znaków na klawiaturze
  np. 123456, qwerty, asdfgh
- sekwencją tych samych znaków np. 33333, aaaaa,
- oparte na ciągu znaków ulegających zmianie w zależności od daty lub innego przewidywalnego czynnika,
- dowolnym elementem spośród wymienionych powyżej z doklejoną na końcu cyfrą lub liczbą.

PBI - instrukcje / procedury

Użytkownicy powinni stosować **łatwe do zapamiętania hasła**, które są jednocześnie **trudne do odgadnięcia**:

1) łącząc kilka słów razem,
2) łącząc znaki przestankowe i cyfry ze słowami,
3) wykorzystując pierwsze litery słów piosenki, wiersza lub innego znanego powiedzenia,
4) celowo stosując słowo z błędem (nie popełnianym jednak często lub nietypowym),

PBI - instrukcje / procedury

5) Szyfr podstawieniowy (klawiatura):

   np. a=s, r=t, e=r, k=l („strl” ☺)

5) Wymiana liter na cyfry lub znaki specjalne:
   a=@, s=$,o=0, B=&, l=1, e=3 np. „@g3ncj@”

6) Dodatki (przedrostki, przyrostki) do haseł w celu zapewnienia unikalności hasła w poszczególnych systemach (hasła modułowe):
   np. „fagl0wn3h@sl019ok”

PODSUMOWANIE

- ✓ Bezpieczeństwo informacji jest ważne w każdej organizacji
- ✓ **Kierownictwo musi się włączyć** w prace nad stworzeniem kultury ochrony informacji
- ✓ Koniecznie należy określić tajemnice przedsiębiorstwa
- ✓ Zabezpieczenia techniczne pomogą, ale nie zastąpią rozsądku
- ✓ Należy zdefiniować **Politykę Bezpieczeństwa Informacji (PBI)**
- ✓ **Szkolenia pomogą** we wdrożeniu i utrzymaniu PBI

PARP Grupa PFR / Centrum Rozwoju MŚP
enterprise europe network
European Commission

DZIĘKUJĘ ZA UWAGĘ … I CIERPLIWOŚĆ

Arkadiusz Stawczyk

W niniejszej prezentacji – jeśli nie wskazano źródła - wykorzystano zdjęcia i grafiki udostępnione przez www.pixabay.com na licencji Pixabay License: „*Darmowy do użytku komercyjnego. Nie wymaga przypisania*”.

ARKADIUSZ STAWCZYK

- trener, doradca i kierownik projektów.
Specjalista w dziedzinie bezpieczeństwa informacji. Egzaminator ECDL oraz kierownik projektów (Fn-TSPM). Specjalista IT Security CISS (Certified IT Security Specialist). Członek Polskiego Towarzystwa Informatycznego. Doradza firmom i jednostkom administracji publicznej m.in. z zakresu ochrony informacji (tworzenie polityk bezpieczeństwa, instrukcji i procedur). Jest autorem licznych instrukcji i procedur związanych z ochroną danych osobowych i informacji. W zakresie szkoleń specjalizuje się w tematach związanych z informatyzacją administracji publicznej, cyberzagrożeniami, bezpieczeństwem informacji i ochroną danych osobowych (Rodo).