Nordea

Anatomia ataku socjotechnicznego

W perspektywie cybernetycznej i komunikacyjnej

Paweł Wawrzyniak, Senior IT Architect

Group Architecture | Technical Solution Architecture

18.03.2019

Nordea Bank Abp SA Oddział w Polsce (cz. I)

Nordea Bank Abp SA Oddział w Polsce wchodzi w skład Grupy Nordea, największej skandynawskiej instytucji finansowej, zatrudniającej ponad 30 000 osób na całym świecie.

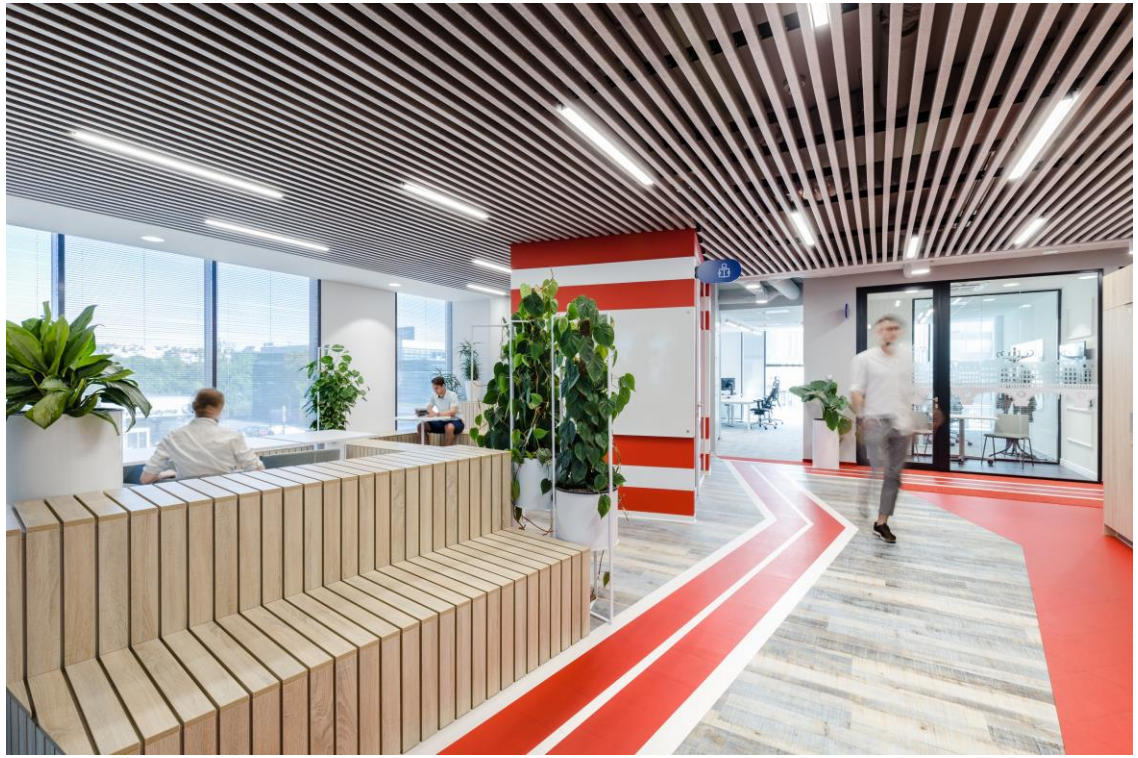
W skład polskiego oddziału wchodzi centrum operacyjne z siedzibą w Łodzi, obsługujące procesy back-officowe dla skandynawskich jednostek biznesowych banku oraz pion IT, zlokalizowany w Trójmieście i Warszawie. Liczba pracowników w obydwu pionach wynosi ponad 3700 osób.

Pion IT w Nordea na co dzień realizuje projekty, których uczestnicy są ulokowani w różnych miejscach w Europie – w Kopenhadze, Sztokholmie, Helsinkach i Oslo. IT w Polsce dostarcza kompleksowe rozwiązania w zakresie utrzymania i rozwoju platform i systemów informatycznych, a obecnie uczestniczy we wdrożeniu jednego z trzech największych systemów bankowych na świecie.

Nordea Bank Abp SA Oddział w Polsce planuje dalszy wzrost zatrudnienia. Wśród poszukiwanych kandydatów są zarówno absolwenci studiów wyższych rozpoczynający ścieżkę kariery, jak i eksperci o ugruntowanej wiedzy informatycznej.

Nordea Bank Abp SA Oddział w Polsce (cz. II)

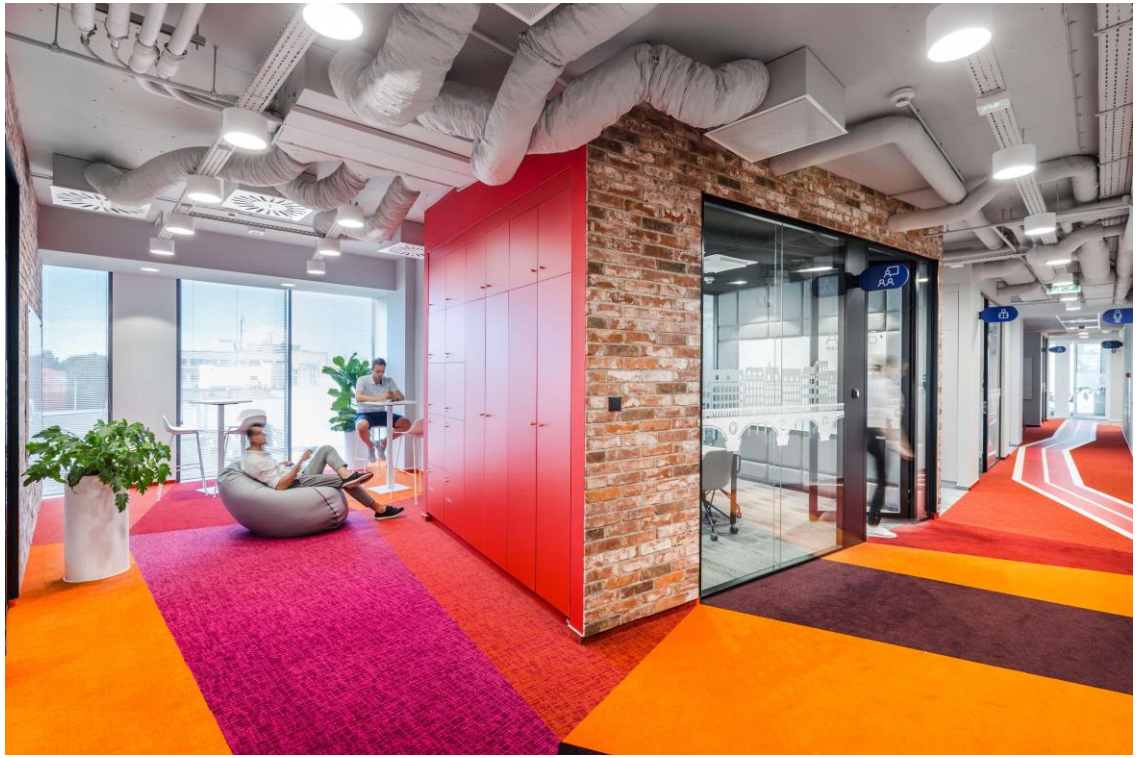
Pracujemy w **najlepszym** biurze w Polsce. Gdyńskie biuro skandynawskiego banku Nordea otrzymało nagrodę w prestiżowym konkursie **Property Design Awards**



Nordea

Nordea Bank Abp SA Oddział w Polsce (cz. III)

Pracujemy w **najlepszym** biurze w Polsce. Gdyńskie biuro skandynawskiego banku Nordea otrzymało nagrodę w prestiżowym konkursie **Property Design Awards**



Nordea

Ataki socjotechniczne. Podstawowe założenia

Najsłabszym ogniwem jest człowiek

- W bankowości – ofiary:
  - Pracownicy (w tym konkretne osoby)
  - Klienci
- W rzeczywistości dotyczą **każdego** z nas
- Nie wymagają zastosowania nowoczesnych technologii (kanałów komunikacji)
- Stanowią istotne wyzwanie w obszarze cyberbezpieczeństwa (**bezpieczeństwa cybernetycznego**)

https://www.seekpng.com/ipng/u2w7q8w7i1w7i1o0_broken-chains-art/

Dlaczego ataki socjotechniczne są ważne? (cz. I)

Raport Europolu Internet Organised Crime Threat Assessment 2018 (IOCTA 2018) **[1]** podaje przykład:

- W marcu 2018 roku, aresztowano w Hiszpanii, w Alicante, przywódcę grupy przestępczej, która przy użyciu złośliwego oprogramowania (ang. *malicious software, malware*) własnej produkcji zaatakowała **ponad 100 instytucji finansowych na świecie**
- Dochodzenie prowadzone było przez policję hiszpańską, przy wsparciu Europolu, FBI, władz rumuńskich, białoruskich, tajwańskich i prywatnych firm zajmujących się bezpieczeństwem cybernetycznym (cyberbezpieczeństwem)

http://m.bankingexchange.com/cyberfraud-id-theft/item/5282-carbanak-cyber-gang-steals-1-billion-from-banks **[2]**

Nordea

Dlaczego ataki socjotechniczne są ważne? (cz. II)

Raport Europolu Internet Organised Crime Threat Assessment 2018 (IOCTA 2018) **[1]** podaje przykład:

- Gang odpowiadał za kampanie **Carbanak** i **Cobalt**, które dotknęły banków w ponad 40 krajach
- Straty oszacowano na ponad **1 miliard EUR**
- Obydwie kampanie zaczynały się od **ataku socjotechnicznego**

http://m.bankingexchange.com/cyberfraud-id-theft/item/5282-carbanak-cyber-gang-steals-1-billion-from-banks **[2]**

Nordea

Czym jest socjotechnika?

- Kevin Mitnick, w książce pt. „**Sztuka** podstępu” **[3]** – definicja negatywna:

> 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**.

- Christopher Hadnagy, w książce pt. „Socjotechnika. **Sztuka** zdobywania **władzy nad umysłami**” **[4]** – definicja prawie neutralna:

> Prawdziwa socjotechnika polega na **manipulowaniu** drugą osobą w taki sposób, aby podjęła **określone działania**, które mogą, ale nie muszą leżeć **w jej interesie**. Może chodzić tu o **pozyskiwanie informacji**, **uzyskiwanie dostępu** do czegoś lub **nakłanianie** ofiary do podjęcia **konkretnych działań**.

Czym jest manipulacja?

- Jerzy Bralczyk, „Manipulacja językowa” **[5]**:

> Dalece nieprecyzyjne definicje manipulacji językowej wiążą ją z takim językowym **działaniem perswazyjnym**, które ma **wpłynąć na postawy** odbiorców (czasem: **sprowokować** ich **działania**) przy założeniu **nieznajomości** (lub **nierozpoznawania**) właśnie stosowanych przez nadawcę zabiegów.

> Manipulację można uznać za **nieetyczną** także w tym sensie, że zawiera **pierwiastek oszustwa**, możliwego dzięki **przewadze nadawcy nad odbiorcą w procesie komunikacji**, gdy warunkiem uczciwej komunikacji jest równość jej uczestników.

- **Język** to system znaków – dalej: **kod** (w szerokim rozumieniu)
- Manipulacja (nie tylko językowa) jest integralną częścią socjotechniki

Czy socjotechnika jest zła? (cz. I)

- Christopher Hadnagy zauważa **[4]**, że:

> Socjotechnika, podobnie jak każde inne narzędzie, **sama w sobie nie jest ani dobra, ani zła** – jest po prostu narzędziem o wielu różnych zastosowaniach.

- Używają jej: dzieci, rodzice, nauczyciele, terapeuci, specjaliści od reklamy i marketingu, sprzedawcy, politycy, stróże prawa i przestępcy… Ktoś jeszcze? ☺

https://pixabay.com/pl/illustrations/w%C5%82%C4%85czenie-grupy-w%C3%B3zek-inwalidzki-2731343/

Czy socjotechnika jest zła? (cz. II)

- Różnice zachodzą w obszarze:
  - intencji i motywacji
  - celu oddziaływania
  - szeroko rozumianego interesu strony oddziałującej i poddawanej oddziaływaniu

https://pixabay.com/pl/photos/strony-marionetka-ba%C5%82wan-polityczny-784077/

Dlaczego cybernetyka?

- **Cybernetyka to nauka o sterowaniu**, zajmująca się ogólnymi modelami sterowania i komunikacji w systemach technicznych, biologicznych i społecznych
- Norbert Wiener, amerykański matematyk – książka pt. „Cybernetyka, czyli **sterowanie** i **komunikacja** w zwierzęciu i maszynie” (1948 r.) **[6]**
- Marian Mazur, twórca polskiej szkoły cybernetycznej, w tym koncepcji **systemów autonomicznych** (autonomów) **[7]**

https://pixabay.com/pl/illustrations/zabezpiecze%C5%84-zamek-pewny-strza%C5%82ki-3014154/

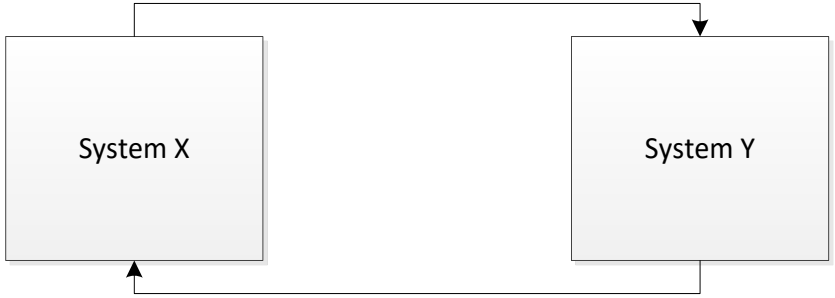
Czym jest sterowanie?

- **Sterowanie jest wywieraniem pożądanego wpływu na określone zjawiska (procesy)**
- W szerszym ujęciu – sterowanie to **oddziaływanie mające na celu** zapewnienie zachowania obiektu w żądany sposób lub w sposób zbliżony do żądanego albo realizację żądanego celu
- Zawsze musi więc istnieć ktoś (lub coś), kto ten wpływ na kogoś (lub coś) wywiera, czyli musi istnieć obiekt sterujący i obiekt sterowany, a także coś, co łączy wzajemnie te obiekty, co umożliwia wywieranie tego wpływu, czyli **kanały** lub po prostu **tor sterowniczy**

https://pixabay.com/pl/vectors/statek-ko%C5%82o-kierownicy-%C5%82%C3%B3d%C5%BA-157789/

Systemy autonomiczne i sprzężenia

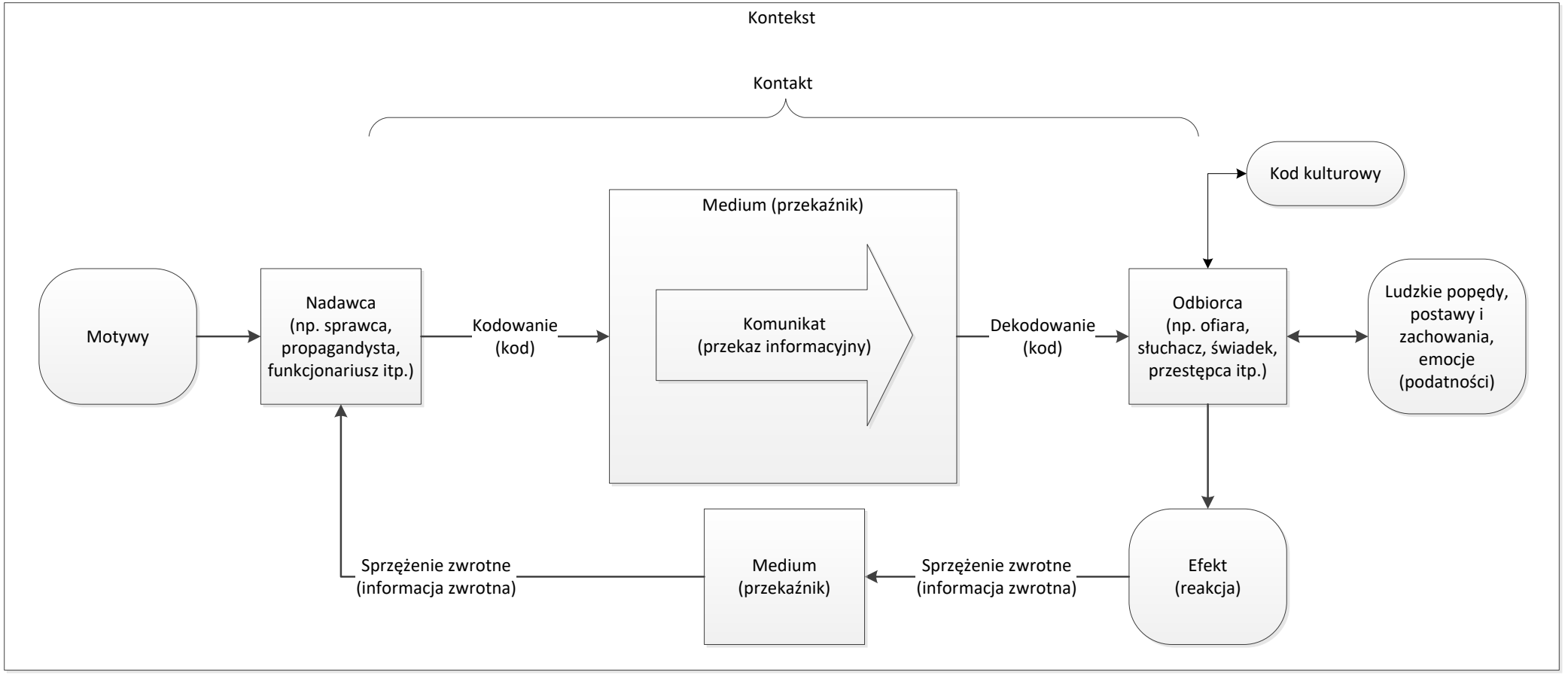
- Zarówno człowieka (jednostkę), jak i społeczeństwo (grupę, zbiorowość) można uznać za **systemy autonomiczne**, czyli takie, które w ogólności mają m.in. **zdolność sterowania się (reagowania) i zdolność przeciwdziałania utracie zdolności sterowania (obrona) oraz funkcjonują we własnym interesie (realizują własne cele)**
- Wszelkie wzajemne oddziaływania pomiędzy systemami możliwe są dzięki istnieniu **sprzężeń**, czyli istniejących między nimi powiązań
- **Sprzężenie, w którym dwa systemy oddziałują na siebie wzajemnie, stanowi sprzężenie zwrotne**



Na podstawie: [7]

Nordea

Atak socjotechniczny jako proces komunikacyjny

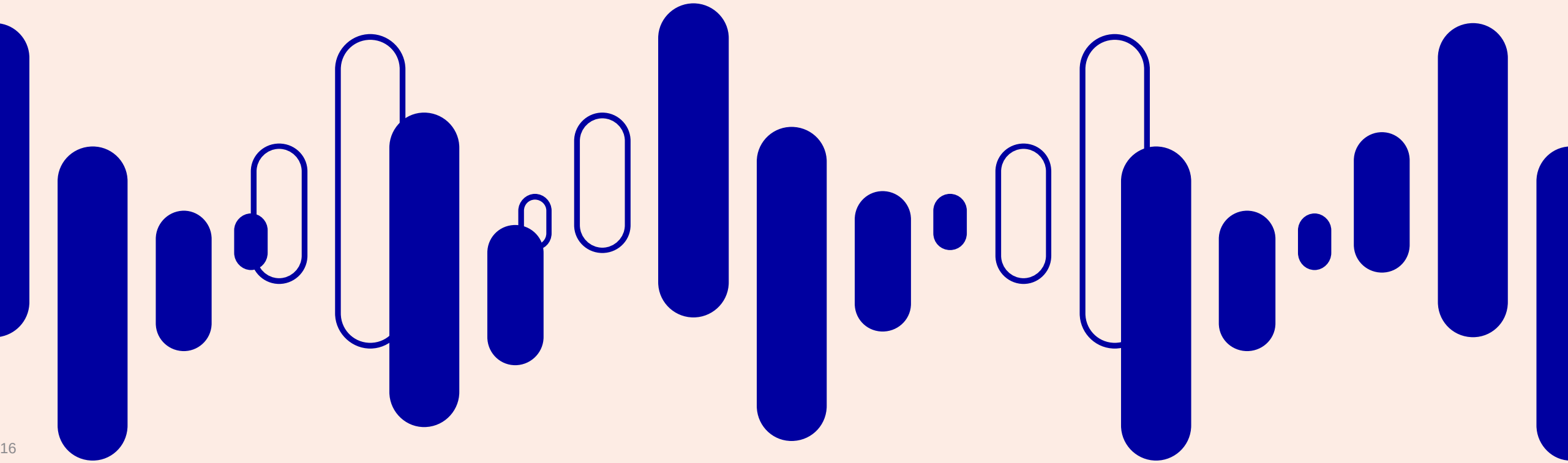


Opracowanie własne na podstawie: **[4], [8]**

Nordea

W praktyce…

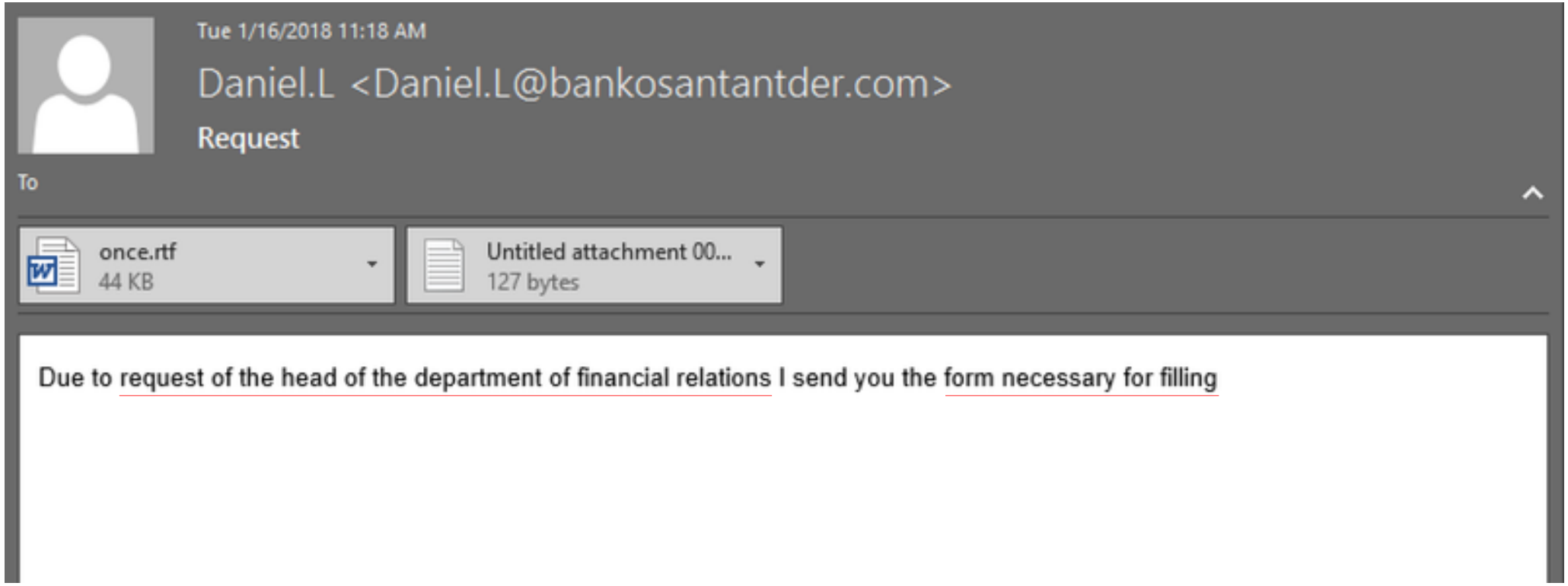
Wybrane przykłady ataków socjotechnicznych



Rodzaje ataków socjotechnicznych

- Najczęściej omawiane ataki:
  - **Phishing** – *password harvesting fishing* (łowienie haseł), charakter masowy
  - **Spear phishing** – atak ukierunkowany na konkretne osoby, wąska grupa odbiorców
  - **Vishing** – *voice phishing*, atak z użyciem połączenie telefonicznego (podszywanie się)
  - **Smishing** – atak z użyciem SMS
  - **Pharming** – szczególny przypadek, bardziej zaawansowany atak
  - […]
- IOCTA 2018 zwraca uwagę, że **phishing** **oparty na poczcie elektronicznej pozostaje najbardziej popularnym cyberatakiem (atakiem cybernetycznym) wykorzystującym socjotechnikę.** Następne w kolejności są warianty tego ataku – tzw. **vishing** i **smishing** **[1]**
- Atak nie musi mieć na celu kradzieży danych (ani haseł)
- Ale to nie wszystko! Socjotechnika jest **wszędzie!**

Spear phishing. Propagacja malware. Kampania Cobalt



Na podstawie: [9]

Nordea

Phishing. Kradzież danych

From: Your Bank <john.smith@john.com>
Sent: Wednesday, March 21, 2018 5:37 PM
To:
Subject: Warning! Account under attack
Importance: High

Dear Customer,

Our system security detected a threat in you account. We have you account deactivated, pending you reactivation immediate. To activate you account again, please Click here and fill out verification form.

If you don't fill in form we will close you account and you many will disappear.

Na podstawie: **[10]**

Nordea

Ransomware. Uśpić czujność ofiary

Na podstawie: **[11]**

Nordea

Smishing

Opracowanie własne

Nordea

Atak na klienta banku metodą „na prokuratora” (cz. I)

- Jeden z wariantów ataku metodą „na wnuczka”:

> Do jednego z mieszkańców zadzwonił telefon.
>
> Mężczyzna w słuchawce przedstawił się z imienia, nazwiska oraz z pełnionej funkcji «prokuratora» nadzorującego prowadzoną właśnie akcję.
>
> «Prokurator» ostrzegł przed oszustami, którzy usiłują wkraść się na konto 85-latka. Podał również pełną instrukcję, w jaki sposób mężczyzna ma zabezpieczyć swoje pieniądze.
>
> Według oszusta jedyną bezpieczną metodą uratowania oszczędności emeryta było wpłacenie ich na podane przez niego (oszusta – przyp. wł.) konto.
>
> «Prokurator» w trosce o bezpieczeństwo mężczyzny nie pozwolił mu się rozłączyć do czasu zakończenia akcji.

Na podstawie: **[12]**

Nordea

Atak na klienta banku metodą „na prokuratora” (cz. II)

- Jeden z wariantów ataku metodą „na wnuczka”:

85-latek udał się do banku, wypłacił 30 tys. zł, cały czas utrzymując kontakt telefoniczny z oszustem i przesłał pieniądze przekazem pocztowym na wskazane konto.

Wtedy oszust poprosił mężczyznę o kolejną kwotę, w celu wsparcia akcji zatrzymania oszustów. Kiedy starszy mężczyzna powiedział, że nie ma więcej oszczędności, oszust zasugerował mu wzięcie w tym celu pożyczki. Mężczyzna będąc przekonany, że pomaga w policyjnej akcji złożył wniosek o przyznanie mu 26 tys. zł kredytu.

Tym razem jednak **czujność i wzorowa postawa pracownika jednego z banków** spowodowała, że do akcji wkroczyli mokotowscy kryminalni, a pokrzywdzony nie przelał sprawcom kolejnych pieniędzy.

(ujęto sprawcę, 25-latka – przy. wł.)

Na podstawie: **[12]**

Nordea

Tailgating, piggybacking… Ogon. Co dalej?

Na podstawie: **[13]**

Nordea

O czym nie rozmawialiśmy?

- Dezinformacja
- Propaganda
- Marketing i sprzedaż
- Wywiad gospodarczy
- Techniczne zaplecze ataków
- Dialog człowieka z maszyną
  - sztuczna inteligencja
  - przetwarzanie języka naturalnego
- Automatyzacja ataków

https://pixabay.com/pl/vectors/g%C5%82owa-g%C5%82owy-ludzi-m%C4%99%C5%BCczyzna-2099128/

Bibliografia

[1] *Internet Organised Crime Threat Assessment 2018 (IOCTA 2018)*, https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf, stan z dn. 18 marca 2019.

[2] J. Ginovsky, *Carbanak cyber gang steals $1 billion from banks. Up to 100 banks victimized in dozens of countries—and cyber scheme remains active*, http://m.bankingexchange.com/cyberfraud-id-theft/item/5282-carbanak-cyber-gang-steals-1-billion-from-banks, stan z dn. 18 marca 2019.

[3] K. Mitnick, *Sztuka podstępu*, przeł. J. Dobrzański, Warszawa 2002.

[4] Ch. Hadnagy, *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, przeł. M. Witkowska, Gliwice 2012.

[5] Jerzy Bralczyk, *Manipulacja językowa* (w:) *Dziennikarstwo i świat mediów*, pod. red. Z. Bauera i E. Chudzińskiego, Kraków 2000.

[6] N. Wiener, *Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie*, Warszwa 1971.

[7] Marian Mazur, *Cybernetyka i charakter*, Warszawa 1976.

Bibliografia

[8] T. Goban-Klas, *Media i komunikowanie masowe. Teorie i analizy prasy, radia, telewizji i Internetu*, Warszawa-Kraków 1999.

[9] Y. Klijnsma, *First Activities of Cobalt Group in 2018: Spear Phishing Russian Banks*, https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/, stan z dn. 18 marca 2019.

[10] *Don't get hooked!*, https://www.nordea.com/en/press-and-news/news-and-press-releases/news-en/2018/2018-03-28-do-not-get-hooked.html, stan z dn. 18 marca 2019.

[11] L. Abrams, *Djvu Ransomware Spreading New .TRO Variant Through Cracks & Adware Bundles*, https://www.bleepingcomputer.com/news/security/djvu-ransomware-spreading-new-tro-variant-through-cracks-and-adware-bundles/, stan z dn. 18 marca 2019.

[12] *Areszt za oszustwo metodą „na prokuratora"*, http://www.policja.pl/pol/aktualnosci/123583,Areszt-za-oszustwo-metoda-quotna-prokuratoraquot.html, stan na dn. 18 marca 2019.

[13] S. Booth, J. Tompkin, H. Pfister, J. Waldo, K. Gajos, R. Nagpal, *Piggybacking Robots: Human-Robot Overtrust in University Dormitory Security*, http://www.eecs.harvard.edu/~kgajos/papers/2017/booth17piggybacking.shtml, stan z dn. 18 marca 2019.

Nordea

Dziękuję