KYBERNETICKÁ BEZPEČNOSŤ

Školenie pre zamestnancov

Nemocnica Alexandra Wintera n.o.
Spracoval D. Dojčan, A. Pernisch

11 sekúnd

NAPADNUTIE

Na svete je každých 11 sekúnd kyberneticky napadnutá spoločnosť.

(Arcserve, 2020)

10 mil. €

STRATY ZA MINÚTU

Každodenná škoda spôsobená kyberzločinom je približne 15 biliónov eur.

(Cybercrime Magazine, 2020)

95%

ĽUDSKÝ FAKTOR

Približne 95% všetkých kyberútokov je zapríčinených ľudským zlyhaním.

(Cyberint, 2020)

TÉMY A CIELE

DEFINOVAŤ PROBLÉM

Určiť problém kybernetickej bezpečnsti a jej dôležitosti.

ROZOZNÁVAŤ HROZBY

Rozoznať skutočné hrozby v on-line priestore od jeho bežných častí.

CHRÁNIŤ SPOLOČNOSŤ

Aplikovať nadobudnuté vedomosti v každodennej praxi.

Hrozba útokov v kybernetickom priestore sa stala tak nebezpečnou, že v r. 2018 Slovenská republika schválila zákon 69/2018 a Vyhlášku 362/2018 o kybernetickej bezpečnosti, kvôli ktorej všetky kritické spoločnosti pre republiku musia spĺnať opatrenia kybernetickej bezpečnosti.

Preto tu dnes aj sedíme, keďže súčasťou sú povinné školenia o kybernetickej bezpečnosti zamestnancov podnikov kritickej infraštruktúry.

VŠEOBECNÝ PRINCÍP SPOCHYBNENIA

PREDPOKLADAŤ HROZBU

Spochybníme podozrivú správu alebo program

Identifikujeme kľúčové časti správy alebo programu

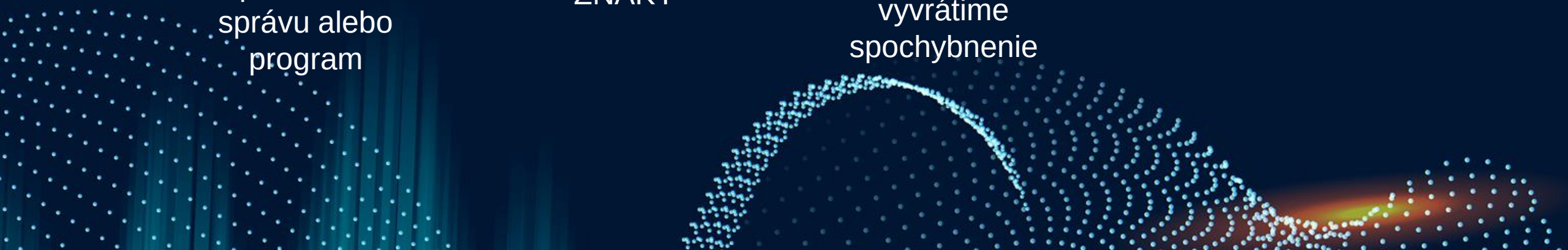
IDENTIFIKOVAŤ ZNAKY

VYVRÁTIŤ SPOCHYBNENIE

Na základe kľúčových častí vyvrátime spochybnenie

Vyhodnotenie vyvrátenia spochybnenia

ROZHODNUTIE



KAŽDODENNÉ ČINNOSTI

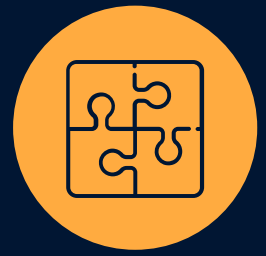
Najslabším článkom kybernetickej bezpečnosti je práve **ľudský faktor**…

E-MAIL

Komunikácia prostredníctvom elektronickej pošty

WWW

Prehliadanie verejných webových stránok



INŠTALÁCIA

Sťahovanie a inštalácia nových programov

KĽÚČOVÉ ČASTI E-MAILU

Prípustné faktory považované za kľúčové

Ako vyzerá falošný e-mail?

A jeho faktory, vďaka ktorým vieme vylúčiť dôveryhodnosť

Logické fauly

Osobné alebo citlivé údaje

Gramatické a syntaxové chyby

Prosím pozor,

Ja som Bar. uchenna ilobi , Ako sa máš, dúfam, že si v poriadku a zdravá? Chceli by sme vás informovať, že som úspešne uzavrel transakciu s pomocou nového partnera z Venezuely a teraz bol fond prevedený do Venezuely na bankový účet nového partnera.

Medzitým som sa rozhodol kompenzovať vás sumou 350 000,00 USD (tristopäťdesiattisíc amerických dolárov) kvôli vášmu úsiliu v minulosti, hoci ste ma v tomto smere sklamali. Ale následne som veľmi rád za úspešné ukončenie transakcie bez akýchkoľvek problémov a preto som sa rozhodol kompenzovať Vás sumou 350 000,00 USD, aby ste sa so mnou o radosť podelili.

Odporúčam vám, aby ste kontaktovali moju sekretárku pre bankomatovú kartu v hodnote 350 000,00 USD, ktorú som si pre vás nechal.
Kontaktujte ho teraz bez zbytočného odkladu.

Názov: šalamúnske brandy

E-mail: solomonbrandyfiveone@gmail.com

Prosím, znova mu potvrďte nasledujúce informácie:

Tvoje celé meno_____ Vaša adresa_____ Tvoja krajina_____ Tvoj vek_____ Vaše povolanie_____
Číslo vášho mobilného telefónu_____

Všimnite si, že ak ste mu neposlali vyššie uvedené informácie úplné, bankomat vám neposkytne, pretože si musí byť istý, že ste to vy.
Požiadajte ho, aby vám poslal celkovú sumu (350 000,00 USD) bankomatovej karty, ktorú som si pre vás nechal.

S Pozdravom,

Pán. uchenna ilobi

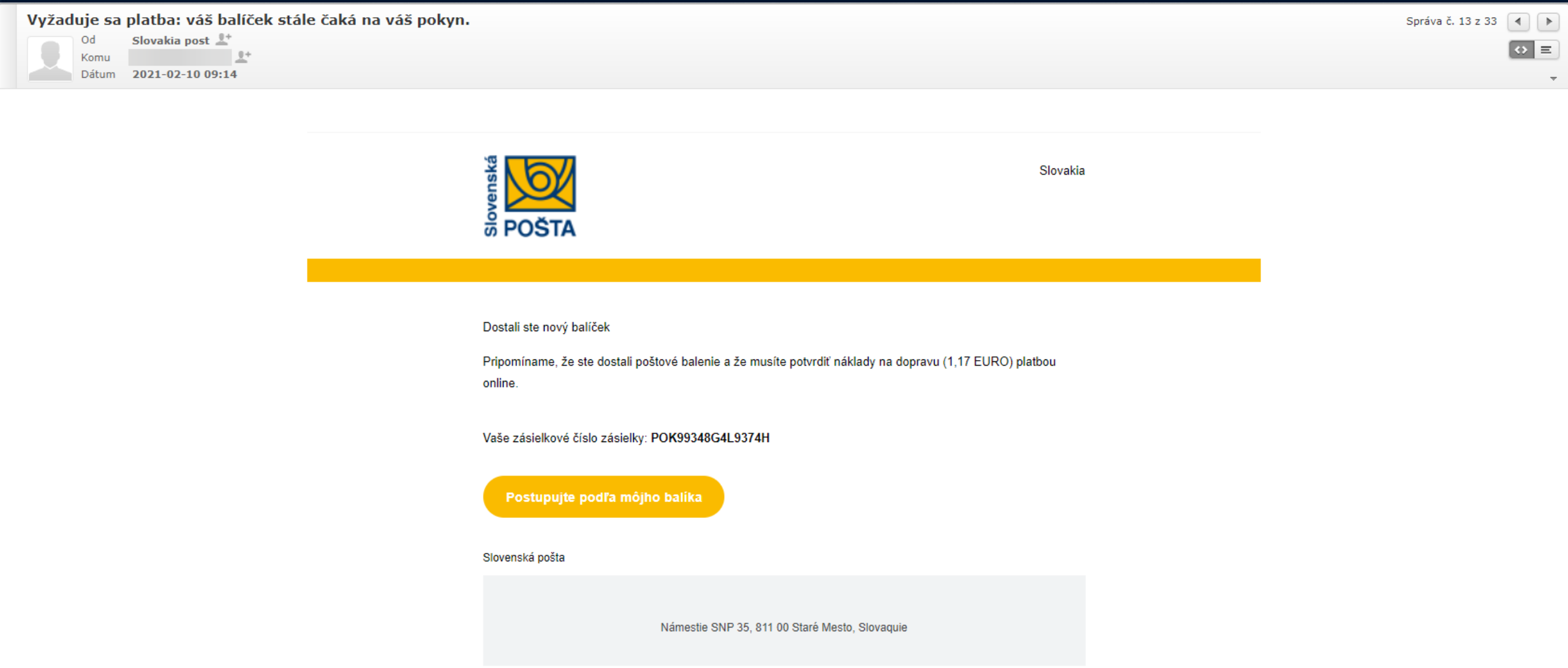
Šokujúce tvrdenia

Finančné či nefinančné odmeny

Logické fauly

Osobné alebo citlivé údaje

Gramatické a syntaxové chyby



Vyžaduje sa platba: váš balíček stále čaká na váš pokyn.

Správa č. 13 z 33

Od Slovakia post

Komu

Dátum 2021-02-10 09:14

Slovenská POŠTA

Slovakia

Dostali ste nový balíček

Pripomíname, že ste dostali poštové balenie a že musíte potvrdiť náklady na dopravu (1,17 EURO) platbou online.

Vaše zásielkové číslo zásielky: **POK99348G4L9374H**

Postupujte podľa môjho balíka

Slovenská pošta

Námestie SNP 35, 811 00 Staré Mesto, Slovaquie

Šokujúce tvrdenia

Finančné či nefinančné odmeny

ČO JE BEZPEČNOSTNÝ INCIDENT?

Bezpečnostný incident je akákoľvek forma kybernetického útoku, ktorá by mohla ohroziť správne fungovanie kritickej infraštruktúry. Môže to byť aj samotný e-mail a pokus o ukradnutie Vašich údajov.

Je toto vaša platná e-mailová adresa?

Od	**Scott.Mckenzie@yukon.ca**
Komu	**Undisclosed recipients:**
Odpovedať na	**info.fluidinves@gmail.com**
Dátum	**St 15:24**

Ahoj,

Potrebujete úver s úrokovou sadzbou 3%? Kontaktujte nás s požadovanou sumou a trvaním.

Ďakujem,

Scott Mckenzie

Ako naložiť s podobným e-mailom?

- V podobnej situácie, ak si nie sme istý o dôveryhodnosti a bezpečnosti e-mailu, odošleme takýto e-mail priamo na IT oddelenie, kde informatici otestujú bezpečnosť a informujú Vás o dôveryhodnosti e-mailu spätnou väzbou.

- Dôležité je na nič neklikať a nesťahovať z podobných e-mailov!

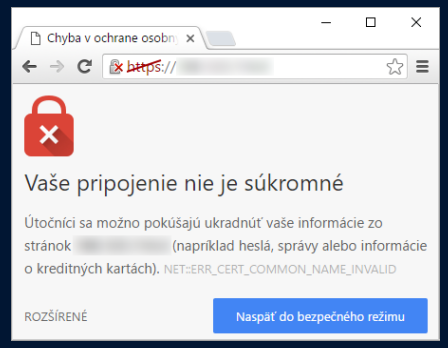
Ransomware

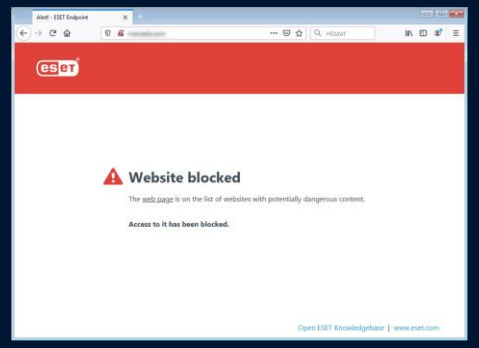
Je najnebezpečnejší typ útoku, ktorý IT svet pozná. Tento vírus sa môže skrývať aj v e-maili, ktorý Vám príde. Môže to byť či už príloha alebo fotka. V priebehu pár minút zničí všetky dáta na sieti.

Ďalšie spôsoby: USB kľúč pohodený na pracovisku, infiltrácia do siete nemocnice, presmerovanie na falošnú webovú stránku

PHISHING – Falošná webová stránka

Najčastejší druh útoku, ktorý sa skrýva väčšinou v e-mailoch. Overiť falošnú kópiu sa dá viacerými spôsobmi. Najčastejšie:





Pozmenenie URL adresy

moja.tatrabanka.sk
moja.t**r**atrabanka.sk
moja.tatrabank**4**.sk

Aj týmto spôsobom môže užívateľ
vytvoriť falošnú kópiu webovej stránky

Nebezpečné stránky

Medzi stránky s potenciálnu hrozbu patria najmä:

1. Stránky s pornografiu
2. Hazardné stránky
3. Zoznamky
4. Stránky nelegálne na Slovensku
5. Stránky s hoax-ami

Správa prístupov

Zjednodušenie cesty do siete útočníka sa skrýva práve pri zlom uchovávaní či úniku prístupov. Z tohto dôvodu by zamestnanci si nemali písať heslá na viditeľné miesta, či do súkromných zariadení a využívať zdieľané účty svojich kolegov.

Pohodený USB kľúč na pracovisku

Z jedných z častých pokusov o infiltráciu je práve tento spôsob.

POKYNY

USB kľúč vziať a nevkladať do pracovného PC, keďže môže skrývať kybernetickú hrozbu.

KONTAKTOVAŤ ŠPECIALISTU

Pri posudzovaní hrozby kontaktovať informatikov pre zaručenie bezpečia a správneho ďalšieho postupu a odovzdať im USB kľúč.

ZÁVER

Informatik určí druh hrozby a následne naloží s USB kľúčom podľa výsledku testovania.

ČO ROBIŤ V PRÍPADE PODOZRENIA NA NAPADNUTIE?

1. Fyzicky odpojiť zasiahnuté zariadenie z internetovej siete, prípadne ho vypnúť
2. Urýchlene nahlásiť podozrenie IT správcom nemocnice

ĎAKUJEME!

Prezentáciu spracoval D. Dojčan a A. Pernisch

Nemocnica Alexandra Wintera n.o.
Winterova 66, 921 01 Piešťany
IČO: 36084221