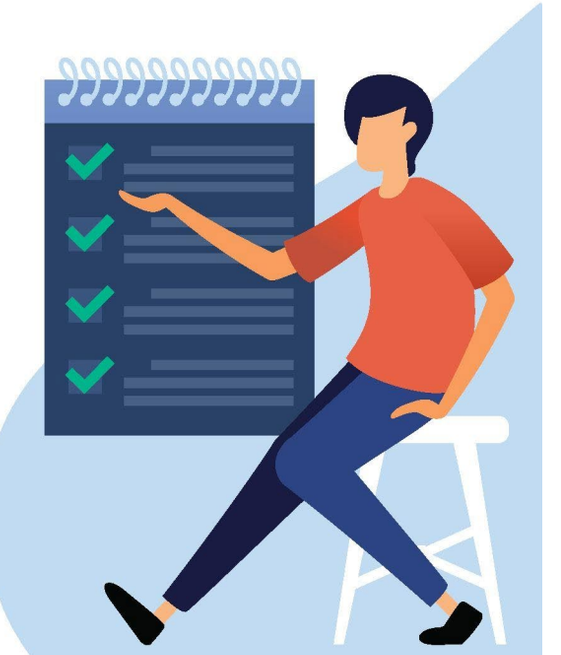
GLOBAL CYBER ALLIANCE

Príručka k súprave GCA Cybersecurity Toolkit for Small Business

Nepoužívajte jednoduché heslá



Aký problém rieši tento panel nástrojov?

Heslá sú prvou obrannou líniou pri ochrane vašich účtov a údajov (ako sú e-maily, záznamy o zamestnancoch alebo databázy klientov).

Bohužiaľ, heslá sú často ľahkým cieľom pre kyberzločincov a k narušeniu údajov hackermi často dochádza práve kvôli slabým heslám. Útočníci poznajú mnoho spôsobov, ako získať prístup k vašim heslám – od použitia ľahko dostupných nástrojov na prelomenie hesiel, čo sú programy, ktoré skúšajú všetky bežne používané kombinácie, až po používateľské mená a heslá získané z napadnutého konta a ich vyskúšanie na iných populárnych stránkach. Tieto techniky si nevyžadujú veľkú technickú zdatnosť, sú rýchle, plne automatizované a sú ľahko dostupné osobám, ktoré si ich vedia vyhľadať na internete. Problémom malých a stredných podnikov je aj to, že mnohé z nich nemajú zavedené pravidlá používania hesiel, alebo ak ich majú, tak ich striktne nevynucujú.

Preto je na ochranu vašich údajov dôležité mať silné heslá. Musíte však ísť ešte o krok ďalej a implementovať dvojfaktorovú alebo viacfaktorovú autentifikáciu (2FA).

2FA vyžaduje viacero overovacích údajov, čo útočníkom sťaží prístup k vašim kontám.

- Pri použití 2FA potrebuje používateľ nasledovné údaje:
- niečo, čo viete, napríklad heslo;
- a niečo, čo máte, napríklad token (Google Authenticator, Authy, Okta, RSA atď.) alebo overovací kód odoslaný na váš telefón; alebo
- niečo, čím ste, napríklad odtlačok prsta alebo tvár (biometria).

Tento panel nástrojov vám pomôže vytvárať silnejšie, jedinečné heslá pre každé z vašich kont a ukáže vám, ako nastaviť 2FA, čo sú dôležité kroky pri ochrane prístupu k vašim kontám a údajom.

Čo vám tento panel nástrojov pomôže dosiahnuť?

Po dokončení tohto panela nástrojov budete lepšie vedieť:

- **ako vytvoriť silné heslo**
- **otestovať svoje kontá a zistiť, či neboli napadnuté**
- **nastaviť 2FA pre väčšinu bežných online kont**

Ako používať panel nástrojov

Pomocou nástrojov na paneli **Nepoužívajte jednoduché heslá** zaistíte, že vaše zariadenia a aplikácie budú mať nastavené silné heslá a 2FA. Ak ste vytvorili inventár v časti „Poznajte svoje prostriedky“, použite ho ako sprievodcu a kontrolný zoznam, aby ste sa uistili, že ste ho implementovali vo všetkých svojich účtoch.

Po dokončení panela nástrojov „Nepoužívajte jednoduché heslá“ aktualizujte svoj kontrolný zoznam zabezpečenia a nastavte pripomenutie pravidelného opakovania tohto procesu, aby sa stal rutinným.

Navigácia v podkategóriách panela nástrojov a ďalšie informácie, ktoré je potrebné zvážiť

3.1 Silné heslá

Jednou z najbežnejších metód, ktoré zločinci používajú na získanie prístupu k vašim účtom, sieti a informáciám, je prihlásiť sa pod vaším menom.
Je naozaj dôležité, aby ste:

- pre každý z vašich účtov používali jedinečné, silné heslo (alebo prístupovú frázu).
- na zabezpečenie silného hesla používali písmená, čísla a špeciálne znaky.
- si okamžite zmenili heslo, ak bolo konto narušené.
- udržiavali svoje heslá v súkromí a bezpečí.
- nikdy znova nepoužívali rovnaké heslo.
- nikdy neklikali na prepojenie v e-maile typu: „Mali by ste obnoviť heslo.“ Vždy pristupujte na webovú stránku účtu cez webový prehliadač.
- sa vyhli prihlasovaniu do účtov cez verejné siete Wi-Fi.

Používanie rovnakého hesla na viacerých účtoch znamená, že ak zločinec získa jedno z vašich hesiel, efektívne získal prístup ku všetkým vašim účtom s daným heslom. Údaje o používateľských menách a heslách môžu predávať na internete zločinci, ktorí ich ukradli v rámci kybernetického útoku, a môžu sa znova používať, až kým sa heslo nezmení. Rýchly technologický pokrok znamená, že aj lacný moderný notebook dokáže rýchlo prechádzať všetkými kombináciami znakov a odhaliť krátke jednoduché heslá.

Mali by ste mať pravidlá používania hesiel, ktorým rozumejú a dodržiavajú ich všetci zamestnanci aj všetci dodávatelia, ktorí majú prístup k vašim systémom. Niektoré systémy a aplikácie umožňujú vyžadovanie minimálneho povoleného hesla, takže sa to určite oplatí skontrolovať v nastaveniach zabezpečenia.

Pomocou nástrojov v časti Silné heslá sa môžete dozvedieť viac o heslách a skontrolovať, či vaša e-mailová adresa nebola napadnutá pri úniku informácií. Ak áno, okamžite si zmeňte heslo a nikdy heslá nepoužívajte opakovane.

Nezabudnite tiež skontrolovať nastavenia hesla aj na smerovačoch, tlačiarňach a iných zariadeniach pripojených k vašej sieti. Na tieto zariadenia možno ľahko zabudnúť a vo všeobecnosti sa dodávajú s jednoduchými predvolenými heslami. Prejdite si inventár, ktorý ste vytvorili v časti „Poznajte svoje prostriedky“, a postupne ich začiarknite.

3.2 Nástroje na 2FA

Dvojfaktorová autentifikácia (2FA) poskytuje okrem hesiel aj dôležitú druhú líniu obrany na ochranu účtov pred neoprávneným prístupom. Existuje množstvo rôznych metód autentifikácie, ktoré možno použiť na 2FA. Tie zahŕňajú napríklad jedinečný kód odoslaný prostredníctvom SMS na váš mobilný telefón, hardvérový token, ktorý nosíte so sebou, odtlačok prsta alebo rozpoznávanie tváre.

Nástroje na 2FA obsahujú zdroje na prevzatie, ktoré poskytujú akceptované metódy overenia pre mnohé bežné účty.

Pri implementácii nástrojov a pokynov na paneli nástrojov „Nepoužívajte jednoduché heslá“ tiež zvážte, aké povolenia bude mať každý používateľ pri prístupe do podnikových aplikácií. Zvážte obmedzenie prístupu len na osoby, ktoré prístup naozaj potrebujú, a v rozsahu, ktorý si ich úloha vyžaduje.

3.3 Správa hesiel

Správcovia hesiel predstavujú spôsob, ako bezpečne uchovávať všetky vaše heslá bez toho, aby ste si museli každé pamätať. To znamená, že si musíte zapamätať iba jedno heslo zakaždým, keď sa chcete prihlásiť do jedného z účtov, ktorého heslo je uložené v správcovi hesiel. Správcovia hesiel poskytujú viac pohodlia. Znamená to však aj to, že ak dôjde k ohrozeniu správcu hesiel, útočník bude mať prístup ku všetkým heslám.

Ďalšie informácie, podpora a usmernenia počas implementácie sú k dispozícii prostredníctvom kategórie **Nepoužívajte jednoduché heslá** na komunitnom fóre GCA.

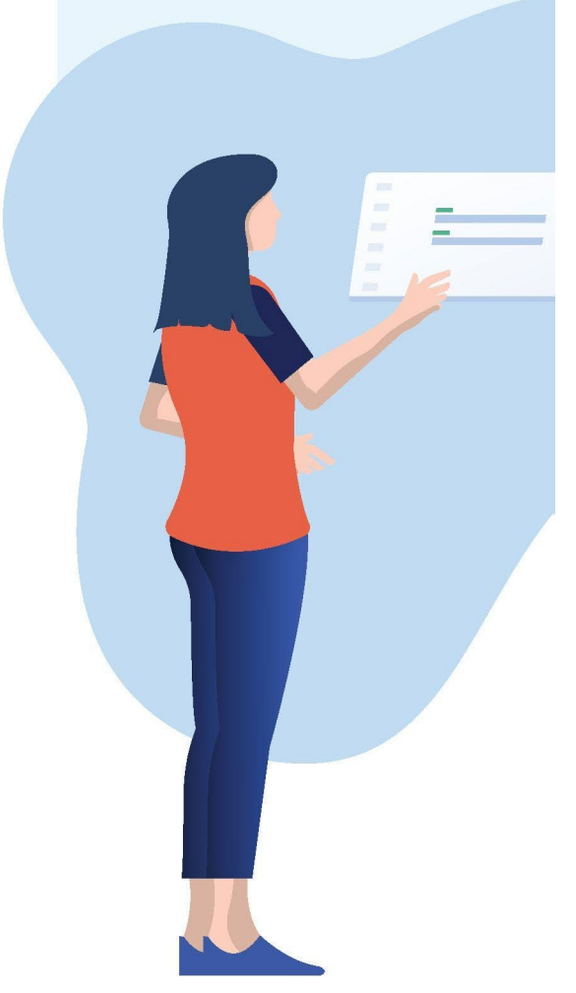
Prepojenia „Nepoužívajte jednoduché heslá“:

Súprava nástrojov: Panel nástrojov „Nepoužívajte jednoduché heslá“

https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/

Komunitné fórum: Kategória „Nepoužívajte jednoduché heslá“

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/beyond-simple-passwords/10



Slovníček pojmov

Slovník niektorých bežne používaných výrazov súvisiacich s kybernetickou bezpečnosťou. Niektoré z týchto pojmov boli uvedené v kapitolách príručky GCA Cybersecurity Toolkit for Small Business, zatiaľ čo iné poskytujeme ako doplnkové informácie, ak si chcete zistiť viac sami.

účet (konto) Vo všeobecnosti označuje prístup k počítačovému systému alebo online službe, pričom na vstup sa zvyčajne vyžaduje heslo.

protivník Osoba, skupina, organizácia alebo úrad, ktorý vykonáva alebo má v úmysle vykonávať škodlivé činnosti.

antivírus Softvér, ktorý je určený na detekciu, zastavenie a odstránenie vírusov a iných druhov škodlivého softvéru.

aplikácia (appka) Program určený na vykonávanie špecifických úloh. Slovo appka často označuje programy stiahnuté do mobilných zariadení.

aktívum Osoba, štruktúra, zariadenie, informácia, záznamy, systémy a zdroje informačných technológií, materiál, proces, vzťahy alebo povesť, ktoré majú nejakú hodnotu. Čokoľvek užitočné, čo prispieva k úspechu niečoho, ako napríklad organizačná misia;
aktíva sú hodnotné veci alebo vlastnosti, ktorým možno priradiť hodnotu.

útok Pokus o získanie neoprávneného prístupu k systémovým službám, zdrojom alebo informáciám, alebo pokus o narušenie integrity systému. Úmyselný akt pokusu o obídenie jednej alebo viacerých bezpečnostných služieb alebo kontrol informačného systému.

charakter útoku Charakteristický alebo typický vzor, ktorý je možné vyhľadať alebo ktorý možno použiť pri porovnávaní s predtým identifikovanými útokmi.

povrch útoku Súbor spôsobov, ktorými môže protivník preniknúť do systému a potenciálne spôsobiť škodu. Vlastnosti informačného systému, ktoré umožňujú protivníkovi preskúmať, zaútočiť alebo udržiavať svoju prítomnosť v informačnom systéme.

útočník Škodlivý protivník, ktorý sa snaží zneužiť počítačové systémy s úmyslom zmeniť, zničiť, ukradnúť alebo znefunkčniť ich informácie a následne zneužiť výsledný stav.

autentifikácia Proces overenia, že niekto je tým, za koho sa vydáva, keď sa pokúša získať prístup k počítaču alebo online službe. Tiež zdroj a integrita údajov, používateľa, procesu alebo zariadenia.

zadné dvere Skrytý spôsob, ako môžu počítačoví zločinci získať neoprávnený prístup k počítačovému systému.

záloha Kópia vašich údajov uložená na inom mieste ako pôvodné údaje, ktorá vám môže pomôcť pri obnove po útoku alebo strate údajov.

zálohovanie Vytvorenie kópie údajov uložených v počítači alebo na serveri, aby sa znížil potenciálny negatívny vplyv zlyhania alebo straty.

bot Počítač alebo zariadenie pripojené k internetu, ktoré bolo tajne napadnuté škodlivým kódom, aby vykonávalo činnosti pod kontrolou vzdialeného správcu.

botnet Sieť infikovaných zariadení (botov), pripojených k internetu, používaných na páchanie koordinovaných kybernetických útokov bez vedomia ich majiteľa.

Slovníček pojmov

narušenie Incident, pri ktorom sú údaje, počítačové systémy alebo siete sprístupnené alebo ovplyvnené neoprávneným spôsobom.

útok hrubou silou Použitie výpočtového výkonu na automatické zadávanie veľkého množstva kombinácií hodnôt, zvyčajne s cieľom odhaliť heslo a získať prístup.

bug Neočakávaná a relatívne malá chyba, porucha, nedostatok alebo nedokonalosť v informačnom systéme alebo zariadení.

konfigurácia Usporiadanie softvérových a hardvérových komponentov počítačového systému alebo zariadenia.

konfigurovanie Proces nastavenia softvéru alebo zariadení pre konkrétny počítač, systém alebo úlohu.

kyberútok Škodlivý pokus poškodiť, narušiť alebo získať neoprávnený prístup k počítačovým systémom, sieťam alebo zariadeniam pomocou kybernetických prostriedkov.

kybernetický incident Narušenie bezpečnostných pravidiel pre nejaký systém alebo službu – najčastejšie pokusy o získanie neoprávneného prístupu k systému a/alebo k údajom, neoprávnené používanie systémov na spracovanie alebo ukladanie údajov, zmeny softvéru alebo hardvéru/firmvéru systému bez súhlasu vlastníkov systému, škodlivé narušenie alebo zamietnutie služby.

kybernetická bezpečnosť Ochrana zariadení, služieb a sietí – a informácií v nich – pred krádežou alebo poškodením.

kryptomena Digitálne peniaze. Kryptomena je uložená v digitálnej peňaženke (online, vo vašom počítači alebo na inom hardvéri). Kryptomena zvyčajne nie je podporovaná žiadnou vládou, takže nemá rovnakú ochranu ako peniaze uložené v banke.

slovníkový útok Typ *útoku hrubou silou*, pri ktorom útočník používa známe slová zo slovníka, frázy alebo bežne používané heslá.

digitálna stopa „Stopa“ digitálnych informácií, ktoré zanecháva online aktivita používateľa.

odmietnutie služby (DoS) Útok, pri ktorom je legitímnym používateľom odmietnutý prístup k počítačovým službám (alebo zdrojom), zvyčajne preťažením služby požiadavkami.

zariadenie Časť počítačového hardvéru, ktorá je navrhnutá na konkrétnu funkciu – napríklad notebook, mobilný telefón alebo tlačiareň.

DMARC Skratka pre Domain-based Message Authentication, Reporting and Conformance. DMARC je mechanizmus, ktorý umožňuje odosielateľom a príjemcom monitorovať a zlepšovať ochranu ich domény pred podvodnými e-mailmi.

spoofing e-mailovej domény Technika používaná počítačovými zločincami, pri ktorej sa použije „sfalšovaná“ e-mailová adresa úplne rovnaká ako pravá, takže sa zdá, že správa bola skutočne odoslaná od danej organizácie.

šifrovanie Konverzia údajov do podoby, ktorá nie je ľahko zrozumiteľná pre neoprávnené osoby.

brána firewall Hardvérové/softvérové zariadenie alebo softvérový program, ktorý obmedzuje sieťovú prevádzku podľa súboru pravidiel o tom, aký prístup je a aký nie je povolený alebo autorizovaný.

hacker Niekto, kto narúša počítačovú bezpečnosť zo zlomyseľných dôvodov, v snahe o slávu alebo osobný zisk.

hardvér Počítač, jeho súčasti a súvisiace vybavenie. Hardvér zahŕňa diskové jednotky, integrované obvody, obrazovky, káble, modemy, reproduktory a tlačiarne.

interná hrozba Osoba alebo skupina osôb s prístupom alebo vnútornými znalosťami spoločnosti, organizácie alebo podniku, ktorá by mohla predstavovať potenciálne riziko porušením bezpečnostných zásad s úmyslom spôsobiť škodu.

internet vecí (IoT) Označuje schopnosť predmetov každodennej potreby (nie počítačov a zariadení) pripojiť sa k internetu. Patria sem napríklad varné kanvice, chladničky a televízory.
narušenie Neoprávnený čin obídenia bezpečnostných mechanizmov siete alebo informačného systému.

Slovníček pojmov

systém detekcie narušenia (IDS) Program alebo zariadenie používané na zistenie, že útočník získal alebo sa pokúsil o neoprávnený prístup k zdrojom počítača.

systém prevencie narušenia (IPS) Systém detekcie narušenia, ktorý pri zistení zablokuje neoprávnený prístup.

keylogger Softvér alebo hardvér, ktorý zvyčajne tajne sleduje stlačenia klávesov a udalosti na klávesnici na sledovanie činnosti používateľa informačného systému.

malvertising Používanie online reklamy ako spôsobu implantovania škodlivého softvéru.

malvér (škodlivý softvér) Pojem, ktorý zahŕňa vírusy, trójske kone, červy alebo akýkoľvek kód či obsah, ktorý by mohol mať nepriaznivý vplyv na organizácie alebo osoby. Softvér určený na infiltráciu a poškodenie alebo deaktiváciu počítačov.

zmiernenie Uplatnenie jedného alebo viacerých opatrení na zníženie pravdepodobnosti nežiaduceho výskytu alebo zmiernenie jeho následkov.

sieť Dva alebo viac počítačov prepojených s cieľom zdieľať zdroje.

externá hrozba Osoba alebo skupina osôb mimo organizácie, ktoré nemajú oprávnenie na prístup k jej aktívam a predstavujú potenciálne riziko pre organizáciu a jej aktíva.

heslo Reťazec znakov (písmená, čísla a iné symboly) používaný na overenie identity alebo overenie oprávnenia na prístup.

prelamovače hesiel Programy určené na uhádnutie hesla, často cyklickým prechádzaním bežne používaných kombinácií alebo použitím používateľského mena a hesla získaného z účtu, ktorý bol napadnutý.

správcovia hesiel Programy, ktoré umožňujú používateľom bezpečne vytvárať, ukladať a spravovať heslá na jednom mieste.

aplikácia záplaty Aplikácia aktualizácií firmvéru alebo softvéru na zvýšenie zabezpečenia alebo zlepšenie funkčnosti.

pentest (penetračné testovanie) Autorizovaný test počítačovej siete alebo systému určený na hľadanie bezpečnostných slabín, aby sa dali opraviť.

osobné identifikačné údaje/osobne identifikovateľné údaje (PII) Informácie, ktoré umožňujú priame alebo nepriame odvodenie identity jednotlivca.

pharming Útok na sieťovú infraštruktúru, ktorý vedie k presmerovaniu používateľa na nelegitímnu webovú stránku napriek tomu, že používateľ zadal správnu adresu.

phishing Necielené hromadné e-maily odosielané mnohým ľuďom, ktoré žiadajú o citlivé informácie (napríklad bankové údaje) alebo ich nabádajú k návšteve falošnej webovej stránky. Digitálna forma sociálneho inžinierstva na oklamanie jednotlivcov, aby poskytli citlivé informácie.

plaintext Nešifrované informácie.

proxy server, ktorý funguje ako prostredník medzi používateľmi a inými servermi a overuje požiadavky používateľov.

ransomvér Škodlivý softvér, ktorý robí dáta alebo systémy nepoužiteľnými, kým obeť nezaplatí.

obnova Činnosti po incidente alebo udalosti na obnovenie základných služieb a prevádzky v krátkodobom a strednodobom horizonte a úplné obnovenie všetkých funkcií z dlhodobého hľadiska.

odolnosť Schopnosť prispôsobiť sa meniacim sa podmienkam a pripraviť sa, vydržať a rýchlo sa zotaviť z narušenia.

obnovenie Obnova údajov po zlyhaní alebo strate počítača.

posúdenie rizika Proces identifikácie, analýzy a hodnotenia rizika spolu s potenciálnymi škodlivými dôsledkami s cieľom formovania priorít, vývoja alebo porovnávania postupov a informovania pri rozhodovaní.

správa bezpečnostných informácií a udalostí (SIEM) Proces, v ktorom sú informácie o sieti agregované, triedené a korelované s cieľom odhaliť podozrivé aktivity.

Slovníček pojmov

smishing Phishing cez SMS – hromadné textové správy odosielané používateľom, ktoré žiadajú o citlivé informácie (napr. bankové údaje) alebo ich nabádajú k návšteve falošnej webovej stránky.

podpis Rozpoznateľný, odlišujúci vzor. Typy podpisov zahŕňajú: podpis útoku, digitálny podpis, elektronický podpis.

sociálne inžinierstvo Manipulácia s ľuďmi pri vykonávaní konkrétnej činnosti alebo prezradenie informácií, ktoré sú pre útočníka užitočné.

softvér Označuje programy na riadenie činnosti počítača alebo spracovanie elektronických údajov.

spam Zneužívanie systémov elektronických správ na rozposielanie nevyžiadaných hromadných správ.

spear-phishing Cielenejšia forma phishingu, keď je e-mail navrhnutý tak, aby vyzeral, že je od osoby, ktorú príjemca pozná alebo ktorej dôveruje.

spoofing Sfalšovanie odosielacej adresy prenosu s cieľom získať nezákonný (neoprávnený) prístup do zabezpečeného systému. Imitovanie identity, predstieranie, piggybacking a napodobňovanie sú formy spoofingu.

spyware Škodlivý softvér, ktorý odovzdáva informácie o činnosti používateľa počítača externej strane.

dodávateľský reťazec Systém organizácií, ľudí, činností, informácií a zdrojov na vytváranie a presun produktov vrátane komponentov produktov alebo služieb od dodávateľov k ich zákazníkom.

systém Vo všeobecnosti označuje systém jeden alebo viacero počítačov alebo zariadení, ktoré zadávajú, vydávajú, spracúvajú a ukladajú údaje a informácie.

správca systému (admin) Osoba, ktorá inštaluje, konfiguruje, rieši problémy a udržiava konfigurácie serverov (hardvér a softvér), aby sa zabezpečila ich dôvernosť, integrita a dostupnosť; tiež spravuje účty, firewally a záplaty; je zodpovedný za kontrolu prístupu, heslá, vytváranie a správu účtov.

hrozba Niečo, čo by mohlo poškodiť systém alebo organizáciu.

aktér hrozby Osoba, skupina, organizácia alebo úrad, ktorý vykonáva alebo má v úmysle vykonávať škodlivé činnosti.

trojan (trójsky kôň) Počítačový program, ktorý je zamaskovaný ako legitímny softvér, no so skrytou funkciou, ktorá slúži na preniknutie do počítača obete. Typ malvéru.

dvojfaktorová autentifikácia (2FA) Použitie dvoch rôznych komponentov na overenie identity používateľa. Označuje sa aj ako viacfaktorové overenie.

virtuálna súkromná sieť (VPN) Šifrovaná sieť často vytvorená na umožnenie bezpečných pripojení pre vzdialených používateľov, napríklad v organizácii s kanceláriami na viacerých miestach.

vírus Počítačový program, ktorý sa dokáže sám replikovať, infikovať počítač bez povolenia alebo vedomia používateľa a potom sa šíriť do iných počítačov. Typ malvéru.

riziko Slabé miesto alebo chyba v softvéri, systéme alebo procese. Útočník môže zneužiť riziko na získanie neoprávneného prístupu do systému.

whaling Vysoko cielené phishingové útoky (maskujúce sa za legitímne e-maily), ktoré sú zamerané na vedúcich pracovníkov.

červ Samoreplikujúci sa, samošíriaci sa, samostatný program, ktorý na svoje šírenie využíva sieťové mechanizmy. Typ malvéru.

Definície boli zostavené z týchto zdrojov:

British Standards Institute

www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

National Cyber Security Centre (NCSC-UK)

www.ncsc.gov.uk/information/ncsc-glossary

National Initiative for Cybersecurity Careers and Studies (NICCS-US)

niccs.us-cert.gov/about-niccs/cybersecurity-glossary

Ďalšie zdroje:

Slovník Australian Cyber Security Centre

www.cyber.gov.au/acsc/view-all-content/glossary

Global Knowledge

www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/

Slovník pojmov zabezpečenia SANS Institute

www.sans.org/security-resources/glossary-of-terms/

Global Cyber Alliance je nezisková organizácia, ktorej cieľom je urobiť z internetu bezpečnejšie miesto znížením kybernetického rizika. Vytvárame programy, nástroje a partnerstvá na zachovanie dôveryhodného internetu s cieľom umožniť sociálny a ekonomický pokrok pre všetkých. GCA je organizácia podľa 501(c)(3) v USA a nezisková organizácia v Spojenom kráľovstve a