GLOBAL CYBER ALLIANCE

Príručka k súprave GCA Cybersecurity Toolkit for Small Business

Vitajte

Vážený kolega:

Internet je dnes neoddeliteľnou súčasťou podnikania väčšiny spoločností. Zabezpečenie digitálneho ekosystému vašej firmy musí byť súčasťou vašej práce. Kybernetický útok môže mať zničujúce následky vrátane finančnej straty, krádeže citlivých informácií, narušenia dodávateľských reťazcov a ďalších dôsledkov.

Určite máte mnoho iných starostí a povinností, tak sme pre vás vytvorili zdroj, ktorý môžete reálne použiť na riešenie problémov v oblasti kybernetickej bezpečnosti.
Súprava nástrojov Global Cyber Alliance (GCA) Cybersecurity Toolkit for Small Business (Súprava nástrojov pre kybernetickú bezpečnosť pre malé podniky) poskytuje bezplatné a efektívne nástroje na zníženie vášho kybernetického rizika. Nástroje sú starostlivo vybrané a usporiadané tak, aby uľahčili vyhľadanie a implementáciu dôležitých krokov, ktoré pomôžu chrániť váš podnik pred kybernetickými hrozbami. Do súpravy sme zahrnuli aj videá, ako aj komunitné fórum, kde môžete nájsť podporu a získať odpovede na otázky od svojich kolegov aj bezpečnostných expertov. Súprava nástrojov je navrhnutá pre vás, nie pre hypotetickú malú firmu so zamestnancami špecializovanými na kybernetickú bezpečnosť a veľkým rozpočtom.

Príručka GCA Cybersecurity Toolkit for Small Business je doplnkom k súprave nástrojov, ktorý vás prevedie jej používaním. Príručku si môžete stiahnuť celú alebo kapitolu po kapitole, keď budete postupovať podľa odporúčaných krokov v súprave nástrojov. Táto príručka vám uľahčí pracovať vlastným tempom pri prijímaní opatrení a bude pre vás užitočným referenčným dokumentom.

Tieto zdroje budú pravidelne aktualizované o vstupy od používateľov, odborníkov z odvetvia a partnerov z celého sveta.

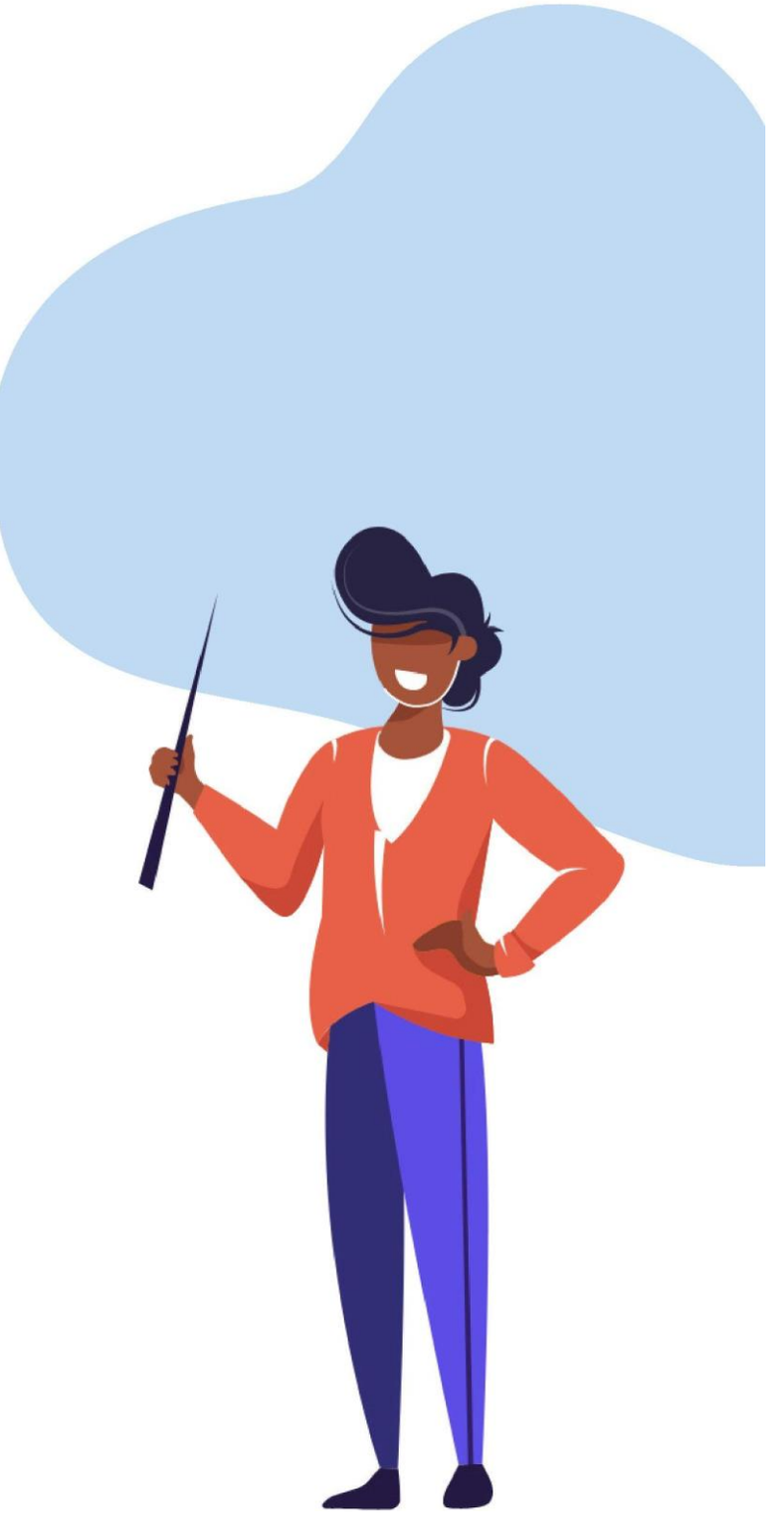
Dúfame, že využijete túto súpravu nástrojov aj príručku na to, aby ste začali zvyšovať svoju kybernetickú bezpečnosť už dnes!

S úctou

Philip Reitinger **PREZIDENT A CEO**

Obsah

Kapitoly príručky



Poznajte svoje prostriedky

Aký problém rieši tento panel nástrojov?

Poznať svoje prostriedky je prvým krokom k lepšej bezpečnosti jednoducho preto, že nemôžete ochrániť to, o čom neviete, že máte. Pamätajte, že mnohé kybernetické útoky a úniky údajov sú spôsobené stratenými alebo ukradnutými notebookmi a inými zariadeniami, neoprávneným prístupom k účtom a neopravenými rizikami v softvéri. Keď budete vedieť, aké počítače, zariadenia a softvér máte (t. j. vaše aktíva), lepšie pochopíte možné riziká, čo vám umožní robiť informované rozhodnutia a podniknúť kroky na zníženie týchto rizík.

- Viete, koľko notebookov a mobilných zariadení má vaša firma, kto k nim má prístup a aký softvér a aplikácie sa na nich nachádzajú?
- Viete, aké staré sú vaše počítače a kedy ste naposledy aktualizovali ich zabezpečenie?
- Máte nejaké systémy alebo zariadenia pripojené na internet (napríklad bezpečnostné kamery alebo ovládacie prvky budovy), ktoré sú tiež pripojené k vašej podnikovej sieti?

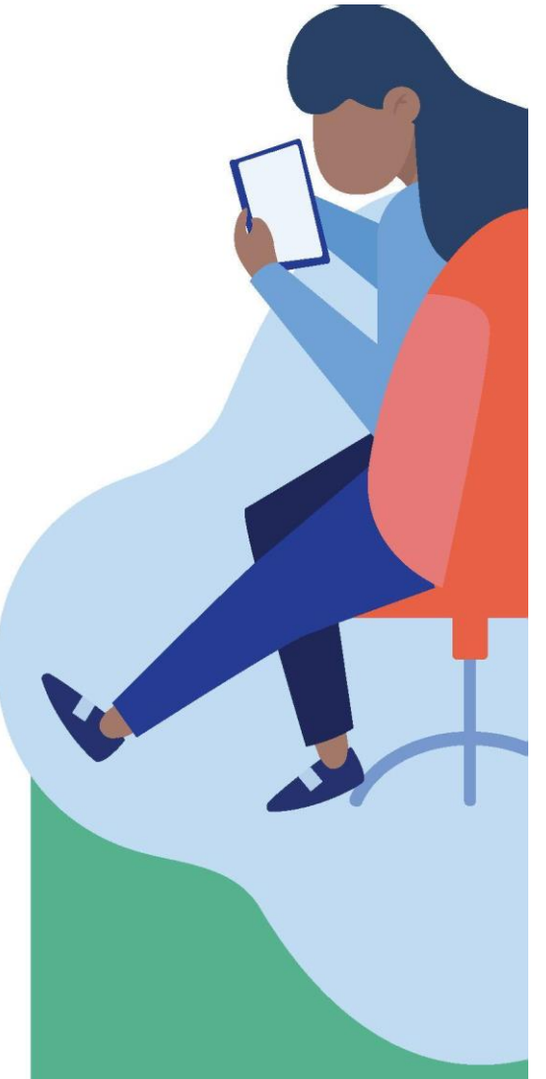
Tieto aktíva môžu byť vektorom prieniku do vášho podnikového prostredia, ktorý by hacker mohol využiť na ukradnutie alebo poškodenie vašich údajov. Je jasné, že je dôležité vedieť, aké zariadenia a systémy máte. Niektoré z vašich aktív sú pre podnikové operácie kritickejšie ako iné a ich úplný a aktuálny zoznam (inventár) vám pomôže určiť priority, čo je potrebné chrániť a na akej úrovni.

Ako používať panel nástrojov

Pomocou nástrojov na paneli **Poznajte svoje prostriedky** môžete identifikovať všetky vaše zariadenia (vrátane stolných počítačov, notebookov, smartfónov a tlačiarní) a aplikácie (napr. e-mail, softvér, webové prehliadače a webové stránky), aby ste mohli podniknúť kroky na ich zabezpečenie.

Tento zoznam vám poslúži ako sprievodca a kontrolný zoznam, keď budete postupne prechádzať ostatnými panelmi nástrojov. Zaistite, aby bol tento zoznam aktuálny, napr. keď pridáte alebo odstránite nové zariadenia, kontá alebo dôležité údaje.

Stiahnite si nástroje z webovej stránky a poznačte si dátumy dokončenia. Využite tiež túto príležitosť a naplánujte si pravidelné kontroly, či sú všetky vaše informácie aktuálne.



Čo vám tento panel nástrojov pomôže dosiahnuť?

Po dokončení tohto panela nástrojov budete lepšie vedieť:

- **ako vykonať inventúru vašich údajov a systémov**
- **ktoré zariadenia a aplikácie sú kritické pre vaše podnikové operácie**

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

1.1 Identifikujte svoje zariadenia

Pri vytváraní inventára je dôležité zvážiť všetko v prostredí vášho podniku. Patria doň položky, ako sú stolné počítače, notebooky, smartfóny, tlačiarne, CCTV, PoS, zariadenia IoT a smerovače.

Mnohé spotrebiteľské zariadenia IoT nemajú žiadne alebo len veľmi minimálne vstavané zabezpečenie, takže zvážte, či je možné ich oddeliť od zvyšku vašej siete alebo ich úplne odstrániť.

Staršie zariadenia môžu už byť mimo záruky, keď už nie sú chránené pred novými rizikami, ale sú stále dôležité pre prevádzku podniku. Mali by ste ich identifikovať v rámci vašej inventúry a vypracovať plán na ich nahradenie, inováciu alebo obmedzenie ich používania.

Pri analýze prostredia IT sa niekedy zabúda na mnohé zariadenia, ako sú smerovače, CCTV a tlačiarne, ale pri inventarizácii aktív by ste mali zvážiť všetko, čo má pripojenie na internet alebo lokálnu sieť, pretože tieto pripojenia často poskytujú potenciálne jednoduchý prienik do vašej firmy.

Identifikujte, kde sa uchovávajú citlivé a dôležité podnikové údaje – či na samostatných zariadeniach pripojených k sieti alebo v cloude. Je možné, že pre tieto zariadenia by sa mali zvážiť ďalšie úrovne ochrany, ale prvým krokom je zdokumentovať, kde je všetko uložené.

1.2 Identifikujte svoje aplikácie

Identifikujte všetky svoje aplikácie vrátane podnikových aplikácií, online účtov, pre ktoré používate svoju firemnú e-mailovú adresu, a ďalších aplikácií, ku ktorým pristupujete lokálne alebo vzdialene prostredníctvom svojich zariadení.

Je dôležité vziať do úvahy všetky aplikácie a účty a pamätať najmä na tie, ktoré už nepoužívate, pretože je nepravdepodobné, že budete ich softvér aktualizovať. Ak už pre vás nie sú nijako užitočné, odstráňte ich alebo zatvorte príslušné účty. Starý online účet môže obsahovať niektoré z vašich osobných údajov a ak dôjde k narušeniu organizácie, pre ktorú ste tento účet pôvodne zriadili, vaše údaje môžu byť ohrozené.

Ďalšie informácie, podpora a usmernenia počas implementácie sú k dispozícii prostredníctvom kategórie **Poznajte svoje prostriedky** na komunitnom fóre GCA.

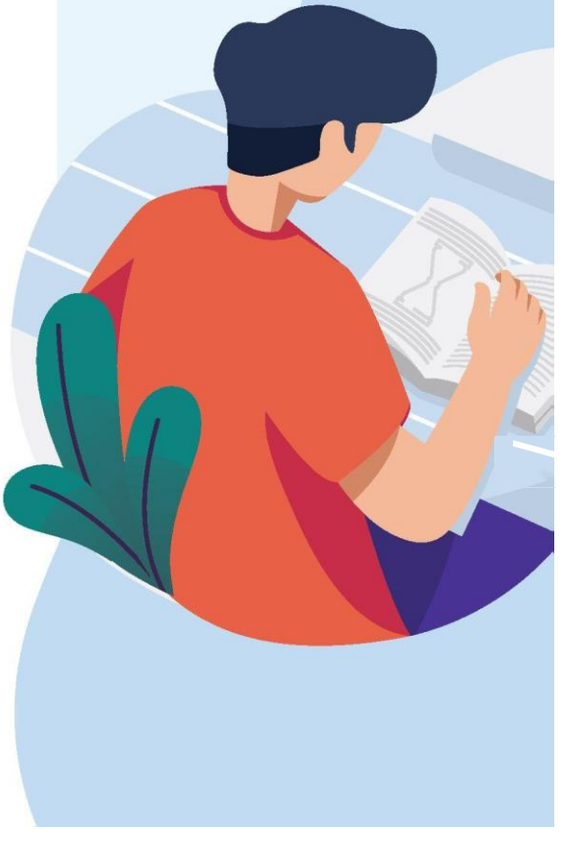
Prepojenia „Poznajte svoje prostriedky“:

Súprava nástrojov: Panel nástrojov… Poznajte svoje… prostriedky

https://gcatoolkit.org/smallbusiness/know-what-you-have/

Komunitné fórum: Kategória „Poznajte svoje prostriedky“

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/know-what-you-have/8



Aktualizujte svoju ochranu

Aký problém rieši tento panel nástrojov?

Kyberzločinci hľadajú slabé stránky a chyby (označované aj ako riziká), pomocou ktorých možno získať prístup k systémom alebo šíriť škodlivý softvér. Zločinci by mohli získať prístup k finančným účtom vašej spoločnosti, údajom vašich zákazníkov a iným citlivým dátam. Môžete sa pred tým chrániť aktualizáciou ochrany (t. j. aktualizáciou systémov, zariadení a údajov). Výrobcovia a vývojári softvéru pravidelne vydávajú bezpečnostné aktualizácie pre svoje operačné systémy a aplikácie, ktoré riešia novoobjavené slabiny alebo riziká. Takéto opravy sa zvyčajne označujú ako záplaty a proces sa označuje ako aplikácia záplaty.

Tento panel nástrojov rieši nutnosť aplikovať takéto záplaty včas vrátane nastavenia (tiež nazývaného konfigurácia) systémov, aby sa dali záplaty aplikovať automaticky vždy, keď je to možné. Okrem toho je dôležité si uvedomiť, že v priebehu času sa mnohé systémy pridávajú, prispôsobujú alebo prestavujú, čo môže viesť k vzniku slabých miest, ktoré by mohli kybernetickí zločinci využiť. Ďalej treba mať na pamäti, či majú prístup k údajom vo vašich systémoch nejakí externí dodávatelia (tretie strany). Uchovávanie aktuálnych záznamov je dôležité; umožňuje vám spravovať aktualizácie zabezpečujúce, aby sa na vaše systémy, zariadenia a aplikácie aplikovali najaktuálnejšie záplaty.

Ako používať panel nástrojov

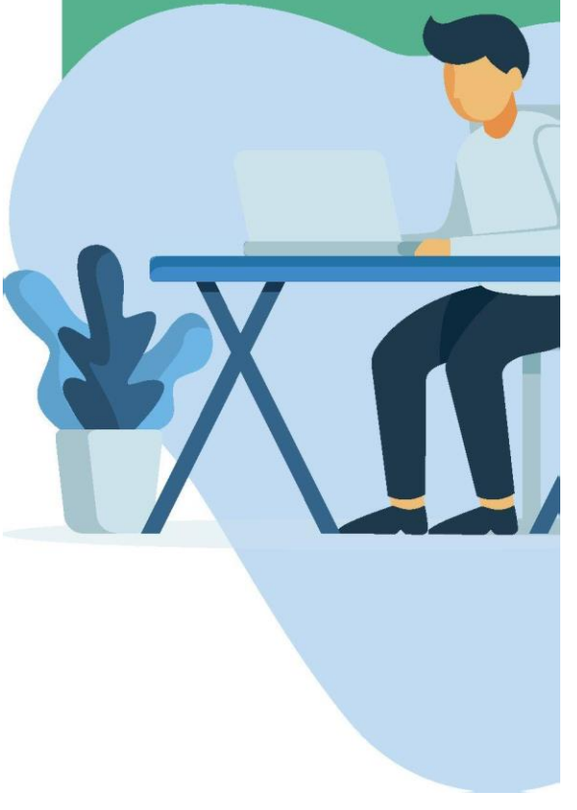
Pomocou nástrojov na paneli nástrojov **Aktualizujte svoju ochranu** zaistíte, že vaše zariadenia a aplikácie budú mať nastavené najnovšie bezpečnostné záplaty a primeranú úroveň zabezpečenia pre typ údajov, ktoré obsahujú. Ak ste vytvorili inventár na paneli nástrojov „Aktualizujte svoju ochranu“, použite ho ako sprievodcu a kontrolný zoznam zabezpečujúci, že všetky vaše zariadenia sú aktualizované a sú nastavené na automatické prijímanie bezpečnostných aktualizácií.

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

Čo vám tento panel nástrojov pomôže dosiahnuť?

Po dokončení tohto panela nástrojov budete lepšie vedieť:

- **skontrolovať, či na svojom zariadení používate najnovšiu verziu softvéru**
- **nastaviť svoje zariadenia tak, aby automaticky prijímali a aplikovali bezpečnostné aktualizácie**
- **implementovať bezpečné konfiguračné nastavenia pre mobilné zariadenia, webové prehliadače a operačné systémy**



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

2.1 Aktualizujte svoje zariadenia a aplikácie

Keď je vytvorené a vydané riešenie alebo záplata na známe riziko, je dôležité, aby všetci používatelia daného systému alebo aplikácie tieto záplaty okamžite aplikovali – ideálne automaticky, pretože kým sa tak nestane, hrozí im narušenie zabezpečenia prostredníctvom tohto rizika.

Skontrolujte každé zariadenie a aplikáciu a nakonfigurujte ich na automatickú aktualizáciu. Vytvorili sme zoznam najbežnejších systémov a aplikácií, ale pre tie, ktoré nie sú zahrnuté v tomto paneli nástrojov, si pozrite pokyny alebo stránky podpory pre konkrétne zariadenie alebo aplikáciu. Začiarknite každú položku zo zoznamu a nezabudnite tento krok vykonať vždy, keď vo svojom podniku pridáte nové zariadenie alebo aplikáciu.

Najbezpečnejšie nastavenia často nie sú nastavené ako predvolené nastavenie zabezpečenia (známe ako konfigurácia) pre vaše zariadenia alebo aplikácie, pretože jednoduchosť používania a pohodlie dostanú často prednosť pred bezpečnosťou. Preto by ste mali skontrolovať, či existujú nejaké výrobcom odporúčané konfigurácie zabezpečenia pre vaše zariadenia a aplikácie a implementovať ich.

Všetky zariadenia, ktoré už nie sú podporované, by sa mali odstrániť, pretože budú vždy vystavené riziku narušenia v dôsledku nejakej novoobjavenej slabiny. Ak to nie je možné, mali by byť izolované od ostatných zariadení a ich používanie by malo byť obmedzené len na špecifické podnikové funkcie.

Nástroje nachádzajúce sa v tomto paneli nástrojov ponúkajú konfiguračný návod k automatickej aplikácii aktualizácií pre bežné systémy. Mali by ste skontrolovať pokyny pre všetky svoje zariadenia a systémy a uistiť sa, že sú správne nastavené.

2.2 Zašifrujte svoje údaje

Ak dôjde k narušeniu vašej počítačovej siete, je vysoká pravdepodobnosť, že hacker bude chcieť ukradnúť citlivé alebo dôverné informácie, ktoré môže použiť na svoje vlastné finančné obohatenie alebo politické ciele. Po zašifrovaní údajov, ktoré sú uložené na vašom pevnom disku, je pre zločincov oveľa ťažšie takéto údaje zneužiť, pretože ich pred použitím bude potrebné dešifrovať.

Šifrovanie je proces, pri ktorom sa údaje konvertujú z čitateľnej formy (t. j. čistého textu) do zakódovanej formy (t. j. šifrovaného textu). Toto zakódovanie je navrhnuté tak, aby bolo nečitateľné pre všetkých okrem osôb, ktoré vlastnia „kľúč(-e)“ na zvrátenie procesu kódovania. Šifrovanie umožňuje zabezpečené ukladanie a prenos údajov, ako aj potvrdenie, že pochádzajú od osoby, ktorá tvrdí, že ich odoslala.

Tieto nástroje vám umožňujú šifrovať súbory uložené na pevnom disku. Ak váš operačný systém nie je na tomto paneli nástrojov uvedený, ďalšie možnosti môžu byť dostupné prostredníctvom výrobcu zariadenia alebo iných komerčne dostupných bezpečnostných ponúk.

2.3 Zabezpečte svoje webové stránky

Pre mnohé firmy je webová stránka rozhodujúca pre fungovanie podniku. Jej používanie môže zahŕňať odosielanie citlivých informácií naprieč dodávateľským reťazcom, alebo môže byť hlavnou obchodnou platformou, na ktorej váš podnik funguje. Ak by hackeri získali prístup do webovej stránky, mohli by zachytiť alebo ukradnúť nejaké údaje, zmeniť jej obsah, infikovať ju škodlivým softvérom alebo prevziať riadenie prevádzky. To môže mať zničujúci vplyv na schopnosť prevádzky vašej organizácie.

Tu nájdete nástroje, pomocou ktorých môžete vykonávať pravidelné kontroly na svojich webových stránkach (tieto kontroly sú známe aj ako skenovanie), aby ste identifikovali riziká a potenciálne slabé miesta. Zabezpečte, aby všetky zistené problémy posúdili kompetentní pracovníci v oblasti IT a prijali príslušné opatrenia.

Podkategórie panela nástrojov obsahujú pokyny a nástroje pre bežne používané systémy. V prípade iných systémov vyhľadajte pomoc na stránke výrobcu alebo na komunitnom fóre GCA **Kategória Aktualizujte svoju ochranu** alebo **Komunita malých podnikov**.

Prepojenia „Aktualizujte svoju ochranu“:

Súprava nástrojov: Panel nástrojov „Aktualizujte svoju ochranu“

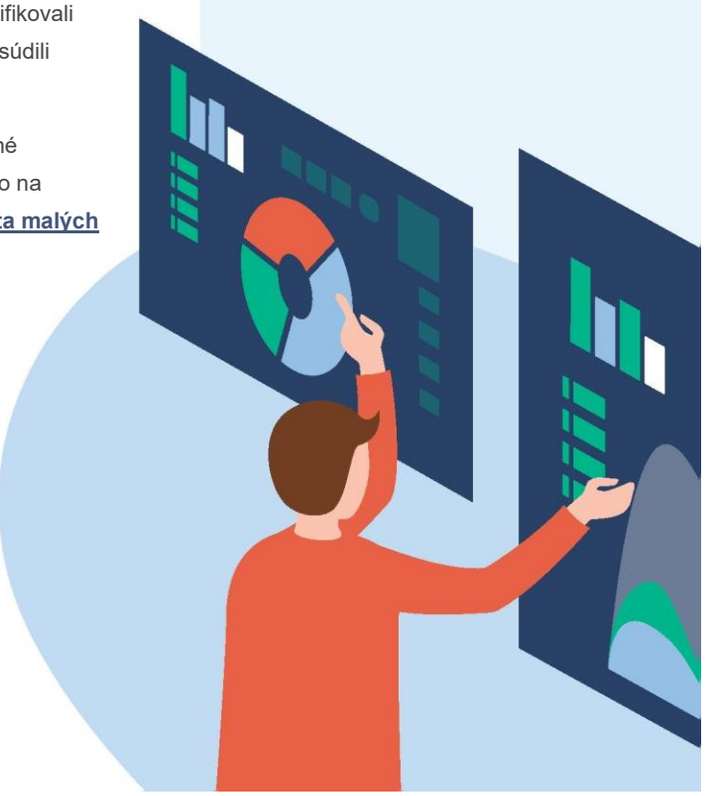
https://gcatoolkit.org/smallbusiness/update-your-defenses/

Komunitné fórum: Kategória Aktualizujte svoju ochranu

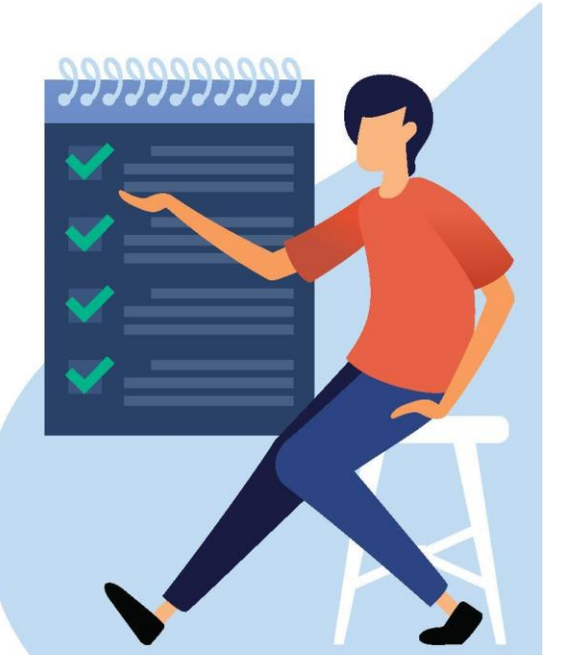
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/update-your-defences/9

Komunita malých podnikov

https://community.globalcyberalliance.org/c/community-discussions/small-business-community/33



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.

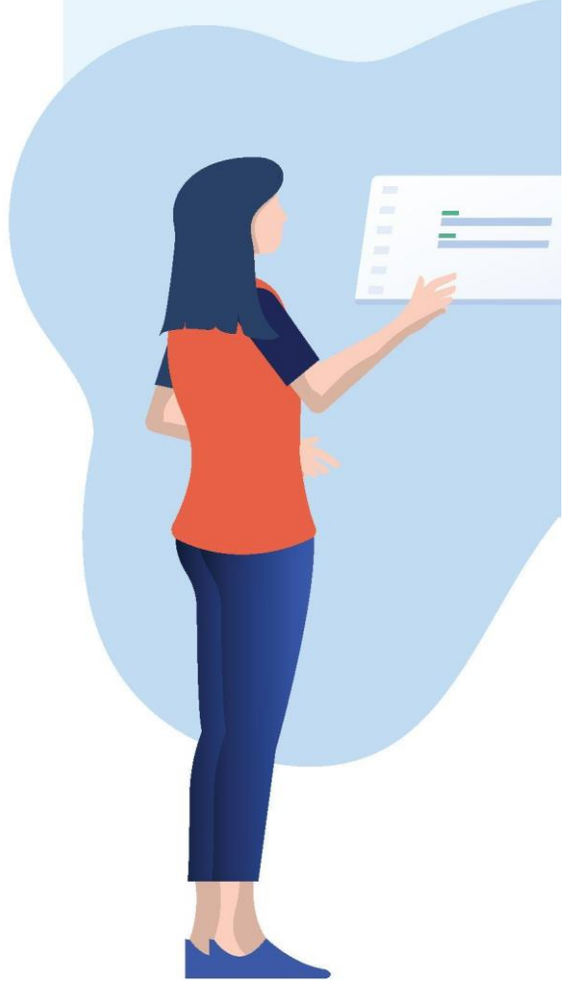
Prepojenia „Nepoužívajte jednoduché heslá“:

Súprava nástrojov: Panel nástrojov „Nepoužívajte jednoduché heslá“

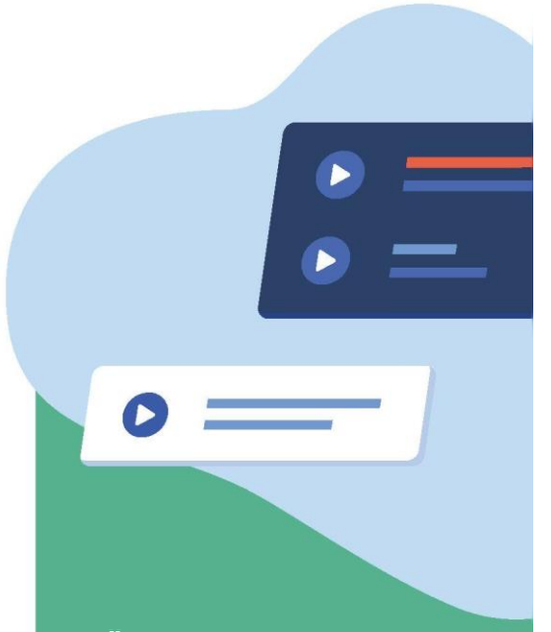
https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/

Komunitné fórum: Kategória „Nepoužívajte jednoduché heslá“

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



Zabráňte phishingu a malvéru



Aký problém rieši tento panel nástrojov?

Každý rok sa mnoho malých podnikov stane obeťou nebezpečných malvérových a phishingových útokov. Keď používateľ klikne na webovú stránku infikovanú škodlivým softvérom (malvérom) alebo otvorí infikovanú prílohu vo phishingovom e-maile, dôsledkom môže byť vymazanie alebo zmena súborov, pozmenenie aplikácií alebo vypnutie funkcií systému.

Malvér je akýkoľvek softvér, ktorý je navrhnutý tak, aby spôsobil poškodenie zariadení alebo sietí či umožnil neoprávnený prístup k nim. Phishingové e-maily používateľa navádzajú, aby uveril, že má dočinenia s dôveryhodným subjektom, takže útočník môže získať neoprávnený prístup k súkromnému, citlivému, obmedzenému obsahu alebo peniazom. Útočník sa snaží, aby jeho e-mail čo najviac vyzeral ako pravý a lákavý, aby prinútil používateľa kliknúť naň alebo otvoriť prílohu. E-maily môžu vyzerať, že pochádzajú od niekoho, koho poznáte, môžu napodobňovať logá a formát e-mailov od známych organizácií alebo môžu odkazovať na najnovšie správy či prácu, ktorú ste práve vykonali.

Niektoré odhady naznačujú, že viac ako 90 % kybernetických útokov sa začína phishingovým e-mailom. Ak kliknete na prepojenie alebo otvoríte prílohu vo phishingovom e-maile, môžete spustiť ľubovoľný počet aktivít, ktoré útočník nastavil a ktoré by mohli zahŕňať krádež vašich údajov, vytvorenie tajnej cesty (známej ako zadné vrátka – backdoor) do vášho počítača na neskoršie použitie, inštaláciu takého typu malvéru, prostredníctvom ktorého vám útočník zablokuje prístup k údajom a požaduje zaplatenie výkupného za prístup k nim (známeho ako ransomvér), alebo stiahnutie iného typu malvéru, ktorý útočníkovi umožní vidieť, čo píšete na klávesnici, ako napr. heslá alebo čísla účtov (známeho ako spyware).

Následky phishingových a malvérových útokov sú pre malé podniky závažné. Dôsledky môžu zahŕňať stratu alebo poškodenie údajov, stratu príjmu, ak sa chod vašej firmy počas útoku zastaví, výdavky vynaložené na opravu/výmenu zariadení, náklady na upovedomenie zákazníkov alebo klientov o narušení, spolu so stratou reputácie a možnými súdnymi spormi.

Panel nástrojov „Zabráňte phishingu a malvéru“ vám pomôže znížiť riziká posilnením vašej odolnosti voči takýmto útokom. Obsahuje nástroje, ktoré vám pomôžu zabrániť navštevovaniu infikovaných webových stránok, antivírusový softvér, ktorý pomôže zabrániť vírusom a inému škodlivému softvéru dostať sa do vášho systému, a blokovače reklám eliminujúce online reklamy, ktoré môžu prenášať vírusy.

Čo vám tento panel nástrojov pomôže dosiahnuť?

Po dokončení tohto panela nástrojov budete lepšie vedieť:

- **ako antivírusový softvér chráni vaše systémy a údaje**
- **ako nainštalovať antivírusový softvér do vášho systému**
- **rozpoznať digitálne reklamy a riziká, ktoré predstavujú**
- **ako nainštalovať blokovač reklám na zablokovanie kontextových reklám, videí a iného neželaného obsahu**
- **čo znamená DNS a prečo je to dôležité**
- **ako funguje zabezpečenie DNS a aké typy útokov eliminuje**
- **ako nainštalovať Quad9 na vaše zariadenia a počítače so systémom Android**

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

Nástroje boli starostlivo vybrané na základe uznávaných globálnych štandardov a nie sú tu uvádzané v žiadnom konkrétnom poradí alebo s odporúčanou prioritou.

4.1 Antivírus

Je dôležité používať antivírus typu „real time“, pretože tento kontroluje vírusy v reálnom čase, keď sa objavia, odstraňuje ich skôr, ako môžu spôsobiť nejaké poškodenie, a aktualizuje sa paralelne s vývojom novej ochrany proti vírusom.

4.2 Blokovače reklám

Niektoré online reklamy alebo správy, ktoré sa zobrazujú pri prehliadaní webových stránok, sú užitočné; iné však môžu obsahovať škodlivý kód a po kliknutí na reklamu by mohli infikovať váš počítač škodlivým softvérom. Blokovače reklám sa môžu použiť na zabránenie zobrazovaniu reklám na webových stránkach a poskytujú tak ďalšiu ochranu pri prehliadaní internetu.

4.3 Zabezpečenie DNS

Zabezpečenie DNS používa systém názvov domén (čo je internetový ekvivalent telefónneho zoznamu) na preklad textového názvu webovej stránky (názov domény), ktorý používateľ zadá do prehliadača, na jedinečný reťazec čísel (IP adresu), pomocou ktorých komunikujú počítače.

Mnoho útočníkov sa pokúša použiť podobné názvy domén webových stránok, aby vytvorili dojem, že sa používateľ pripája k legitímnej stránke. Tieto stránky môžu vyzerať ako skutočná príslušná webová stránka, no pri bližšom preskúmaní môžete objaviť rozdiely.

Takže napríklad legitímna adresa URL webových stránok nejakej spoločnosti môže vyzerať takto:
„www.mygreatwidgets.com,“ ale falošná môže vyzerať takto:
„www.rnygreatwidgets.com.“

Brány firewall DNS, ktoré sú jedným z typov zabezpečenia DNS, môžu pomôcť predchádzať vírusom a phishingovým útokom, pretože kontrolujú, či adresa IP požadovanej webovej lokality neobsahuje škodlivý kód, a ak áno, zablokujú k nej prístup. Používatelia môžu implementovať služby filtrovania DNS na svojich systémoch pomocou nástrojov v rámci tejto podkategórie, aby pomohli zabrániť prístupu k známym škodlivým webovým stránkam.

Podkategórie panela nástrojov obsahujú nástroje pre bežne používané systémy.
Ak potrebujete ďalšiu podporu, vyhľadajte ju alebo sa opýtajte na komunitnom fóre GCA kategórie **Zabráňte phishingu a malvéru** alebo **Komunita malých podnikov**.

Prepojenia „Zabráňte phishingu a malvéru“

Súprava nástrojov: Panel nástrojov „Zabráňte phishingu a malvéru“

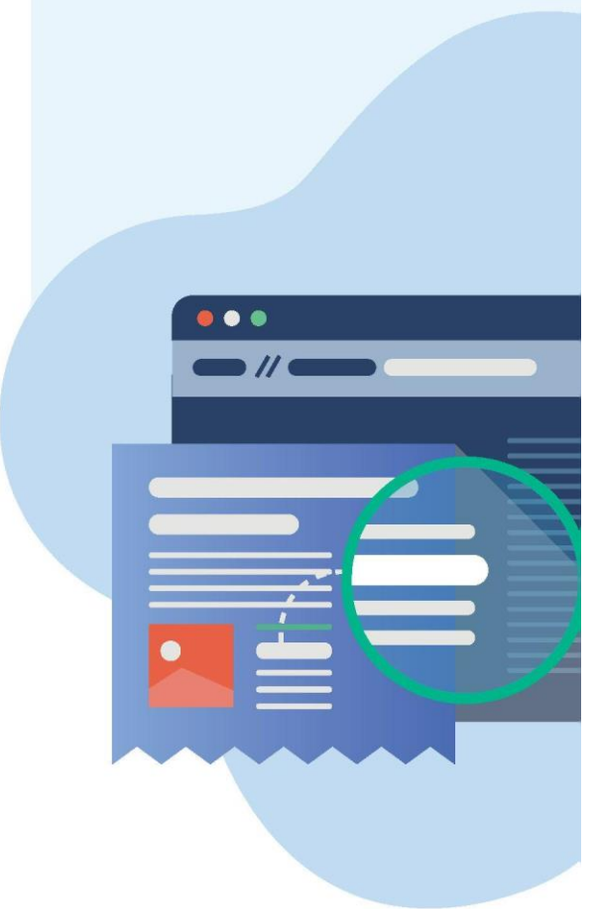
https://gcatoolkit.org/ smallbusiness/prevent-phishing- and-malware/

Komunitné fórum: Kategória „Zabráňte phishingu a malvéru“

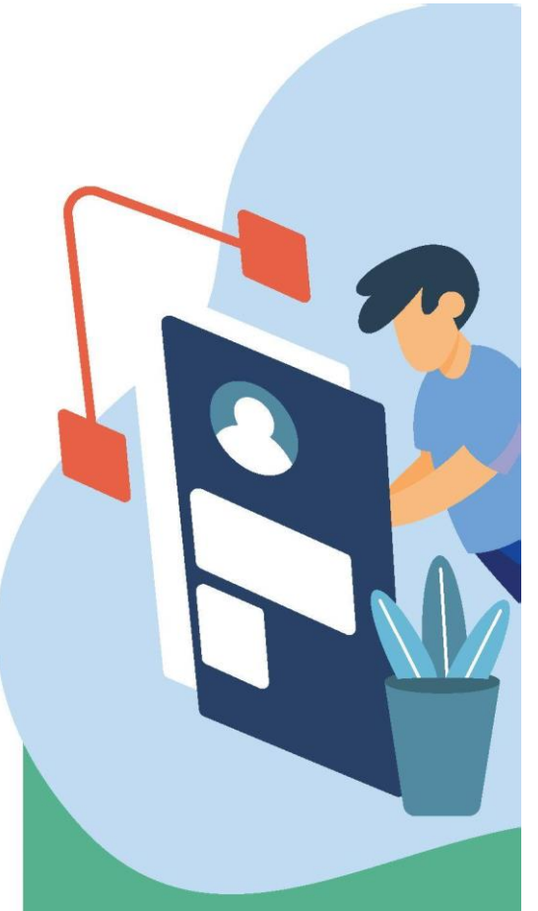
https://community. globalcyberalliance.org/c/ cybersecurity-toolbox/prevent- phishing-and-viruses/11

Komunita malých podnikov

https://community. globalcyberalliance.org/c/ community-discussions/small- business-community/33



Zálohovanie a obnova



Aký problém rieši tento panel nástrojov?

Strata alebo poškodenie údajov môže byť spôsobené kybernetickým útokom (napríklad ransomvérom) alebo zlyhaním či krádežou zariadenia, ľudskou chybou, náhodným poškodením, požiarom alebo záplavou. Bez ohľadu na príčinu môže strata údajov alebo výpadok zariadení vážne ovplyvniť produktivitu a ziskovosť vašej firmy.

Záloha je kópia vašich údajov uložená na inom mieste ako pôvodné údaje a môže vám pomôcť pri obnove po útoku alebo strate údajov. Pravidelné online a offline zálohovanie uľahčuje rýchlejšie zotavenie zo straty alebo poškodenia údajov. Obe sú dôležité, pretože online zálohovanie je nastavené tak, aby sa automaticky zálohovalo cez sieť, zatiaľ čo offline zálohovanie vyžaduje pripojenie a následné odpojenie externého zariadenia (napr. USB alebo pevného disku) na fyzické uloženie údajov inde (čo tiež pomáha predchádzať neúmyselnému zálohovaniu poškodených údajov).

Ako používať panel nástrojov

Pomocou nástrojov na paneli **Zálohovanie a obnova** zabezpečte pravidelné zálohovanie vašich systémov na príslušnej úrovni a s frekvenciou vhodnou pre typ údajov, ktoré sú v nich uložené.

Čo by ste mali zálohovať? To závisí od vašich informácií a rizika straty týchto informácií. Ak ste vytvorili inventár na paneli nástrojov „Poznajte svoje prostriedky“, použite ho ako sprievodcu a kontrolný zoznam, ktorý priebežne aktualizujete.

Po dokončení práce s panelom nástrojov „Zálohovanie a obnova“ aktualizujte svoj kontrolný zoznam zabezpečenia a nastavte si pripomenutie jeho pravidelnej kontroly, aby ste zabezpečili, že vaše pravidlá sú stále vhodné pre vašu firmu.

Čo vám tento panel nástrojov pomôže dosiahnuť?

Po dokončení tohto panela nástrojov budete lepšie vedieť:

- **prečo je zálohovanie dôležité pre váš podnik, najmä pri obnove po útoku pomocou ransomvéru**
- **ako povoliť úplné zálohovanie na počítači so systémom Windows alebo Mac**

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

Ransomvér je jedna z metód útoku, ktorá sa stala vážnym problémom pre malé podniky. Ransomvér je typ škodlivého softvéru, ktorý infikuje počítače a zablokuje prístup k údajom. Páchateľ požaduje platbu, niekedy vo forme kryptomeny (t. j. bitcoinov, ktoré je ťažšie vystopovať ako tradičné prevody), za prísľub, že po prijatí výkupného budú údaje obnovené. Zálohovanie vašich údajov je dôležitou ochranou pre prístup k vašim údajom, ak ste sa stali obeťou ransomvéru.

5.1 Zálohovanie operačných systémov

Kvalitne nastavené pravidlá zálohovania, ktoré zahŕňajú online aj offline zálohovanie, uľahčujú rýchlejšie zotavenie zo straty alebo poškodenia údajov.

- Rôzne skupiny údajov, ktoré uchovávate, by mali byť kategorizované v rámci inventára (pomoc pri vytvorení inventára nájdete na paneli nástrojov „Poznajte svoje prostriedky“).
- Zvážte aj použitie šifrovania pre citlivé informácie (ďalšie informácie o šifrovaní nájdete na paneli nástrojov „Aktualizujte svoju ochranu“).
- Implementujte rozumný prístup k zálohovaniu každej skupiny údajov s prihliadnutím na „vplyv straty“ každej z nich. Vplyv straty môže byť reputačný, finančný alebo právny.

V podkategórii Zálohovanie operačných systémov nájdete návod na zálohovanie na bežných operačných systémoch. Ak váš systém nie je v zozname uvedený, skúste vyhľadať pomoc na webovej stránke vášho poskytovateľa alebo v kategórii **Zálohovanie a obnova** na komunitnom fóre GCA.

Tiež sa uistite, že máte plán obnovy po havárii, ktorý pomáha vykonať obnovu kritických systémov po ich zlyhaní (po nehode alebo prírodnej katastrofe). Mať takýto plán pomáha minimalizovať čas obnovy a poškodenie systémov, chráni pred potenciálnymi právnymi dôsledkami a môže tiež zvýšiť bezpečnosť. Na internete je k dispozícii veľa šablón a návodov na vypracovanie takéhoto plánu. Nezabudnite ho aktualizovať, realizujte aj fiktívne scenáre na vykonanie tohto plánu a ubezpečte sa, že každý vie, ako ho implementovať.

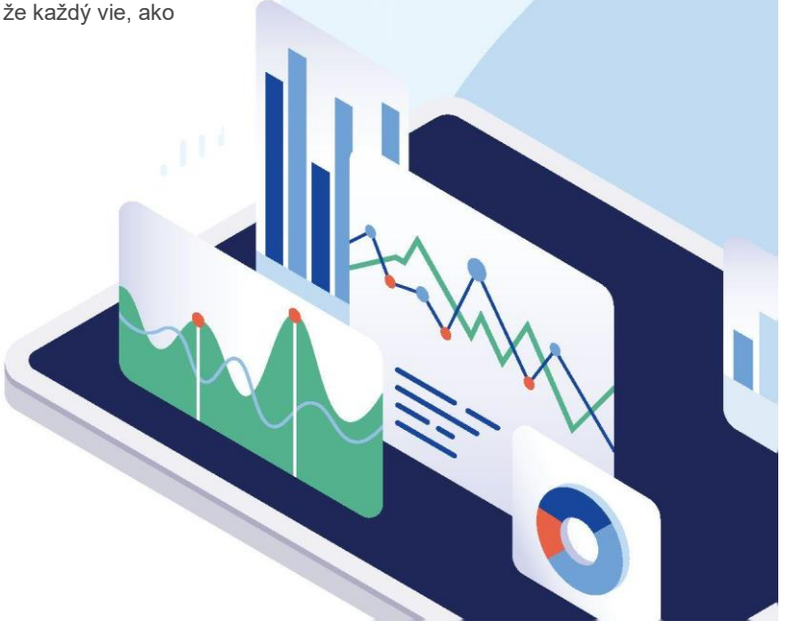
Prepojenia „Zálohovanie a obnova“

Súprava nástrojov: Panel nástrojov „Zálohovanie a obnova“

https://gcatoolkit.org/smallbusiness/backup-and-recover/

Komunitné fórum: Kategória „Zálohovanie a obnova“

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/back-up-and-recover/16



Chráňte svoje e-maily a povesť podniku

Aký problém rieši tento panel nástrojov?

E-mail sa často používa ako východiskový bod pre kybernetický útok. Je mimoriadne rýchle a lacné rozposlať tisíce e-mailov nič netušiacim príjemcom a potom čakať, že aspoň niektorí používatelia kliknú na prepojenie na škodlivú webovú stránku alebo si stiahnu škodlivú prílohu.

Jednou z techník, ktoré kyberzločinci používajú, je e-mail, ktorý vyzerá, ako keby bol odoslaný z legitímneho zdroja, ako je napríklad vaša banka, klient, obchodný partner alebo iná známa organizácia. Jedna z týchto techník je známa ako spoofing e-mailovej domény, pri ktorej je použitá „sfalšovaná“ e-mailová adresa úplne rovnaká ako pravá, takže sa zdá, že správa bola skutočne odoslaná z tejto organizácie, vďaka čomu nemá príjemca dôvod na podozrenie, že tomu tak v skutočnosti nie je.

Ak je e-mailová doména vašej spoločnosti (časť vašej e-mailovej adresy za znakom „@“) sfalšovaná, môže to mať vážne následky pre vás, vašich zákazníkov a dodávateľský reťazec. Ak príjemca e-mailu vykonal nejaký krok v súvislosti s e-mailom, pretože skutočne veril, že pochádza od vás, mohlo by to viesť k infikovaniu jeho počítačového systému nejakou formou malvéru alebo ransomvéru. Mohlo by to tiež umožniť zločincovi prevziať kontrolu a manipulovať s vašimi bankovými údajmi, takže zákazníci budú posielať platby na iné účty mysliac si, že platia vám.

Panel nástrojov „Chráňte svoje e-maily a povesť podniku“ poskytuje návod a nástroje na ochranu pred týmto typom hrozby vrátane predstavenia e-mailového štandardu známeho ako DMARC (Domain-based Authentication, Reporting and Conformance). DMARC je účinný spôsob, ako zabrániť spamerom a phisherom vo využívaní firemných domén na vykonávanie nebezpečných kybernetických útokov. Je to spôsob, ako overiť, či má odosielateľ e-mailu povolenie používať vašu e-mailovú doménu a odosielať e-maily.

Útočníci môžu tiež vytvárať „napodobeniny“ webových stránok. Napríklad pravá doména „BestBusiness.com“ môže byť napodobnená registráciou „BestBusness.com“ alebo „BestBusiness.net“ s cieľom oklamať zákazníkov alebo používateľov, aby ich navštívili.

Ak sú vaše e-mailové alebo webové domény sfalšované, môže to mať za následok poškodenie vašej povesti a značky, ako aj poškodenie vašich zákazníkov. Používanie nástrojov v časti „Chráňte svoje e-maily a povesť podniku“ pomáha identifikovať a predchádzať odcudzeniu identity.

Čo vám tento panel nástrojov pomôže dosiahnuť?

Po dokončení tohto panela nástrojov budete lepšie vedieť:

- **čo znamená štandard DMARC, prečo je dôležitý a akým útokom zabraňuje**
- **ako použiť Sprievodcu nastavením DMARC**
- **ako skontrolovať svoju vlastnú e-mailovú doménu a zistiť, či je aktivovaný štandard DMARC**

Ako používať panel nástrojov

Pomocou nástrojov na paneli **Chráňte svoje e-maily a povesť podniku** zabezpečíte, aby bola vaša spoločnosť chránená pred falšovaním e-mailových domén prostredníctvom implementácie štandardu DMARC, a budete vedieť identifikovať potenciálne napodobeniny domén webových stránok.

Po dokončení aktualizujte svoj kontrolný zoznam zabezpečenia a odporúčajte svojim zákazníkom a dodávateľom, ktorí používajú svoju vlastnú doménu, aby urobili to isté, pretože účinnosť štandardu DMARC závisí od toho, či odosielateľ aj príjemca majú DMARC implementovaný.

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

6.1 Implementácia DMARC

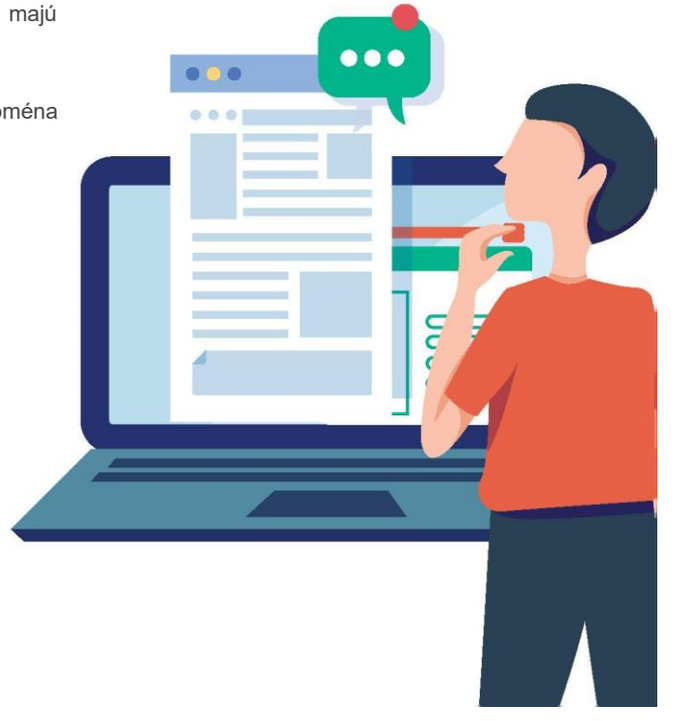
Pomocou nástrojov v tejto podkategórii sa dozviete viac o štandarde DMARC, skontrolujete, či je vaša e-mailová doména chránená štandardom DMARC, a ak áno, na akej úrovni.

6.2 Pochopenie správ DMARC

Po nastavení pravidiel DMARC vo vašej e-mailovej doméne začnete dostávať správy o tom, ako sa vaša e-mailová doména používa. Tieto správy je ťažké narušiť v ich nespracovanom (raw) formáte.

Nástroje v podkategórii „Pochopenie správ DMARC“ pomáhajú pri interpretácii a rýchlejšej identifikácii podvodných aktivít. To vám umožňuje s istotou stanovovať úrovne pravidiel od „žiadnej hrozby“ cez „karanténu“ až po najvyššiu úroveň „zamietnutie“. Je tiež dôležité vziať do úvahy aj všetky e-mailové organizácie alebo služby oprávnené odosielať e-maily vo vašom mene, ako sú e-mailové marketingové služby, a skontrolovať, či majú implementovaný štandard DMARC.

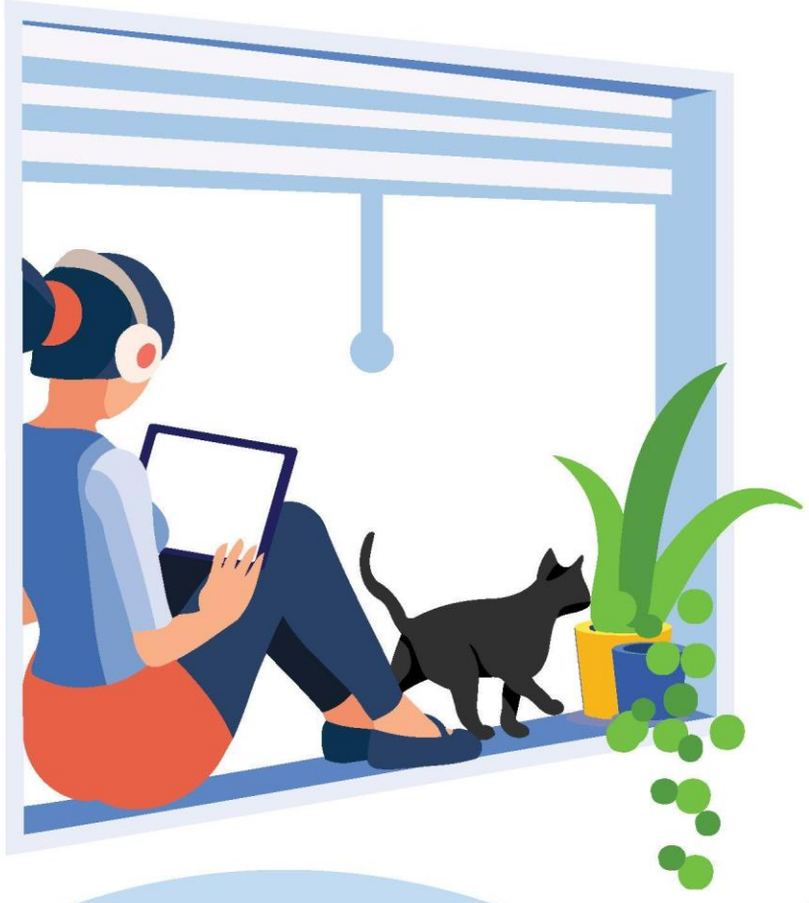
Výhody štandardu DMARC sa naplno prejavia iba vtedy, keď je vaša e-mailová doména v stave „zamietnutie“ (reject).



6.3 Ochrana obchodných značiek

Podvodníci si môžu zaregistrovať domény, ktoré vyzerajú veľmi podobne ako vaša vlastná doména, s cieľom oklamať ľudí, aby na ne klikli. Pomocou nástrojov na tomto paneli môžete identifikovať domény, ktoré sa pokúšajú napodobniť tú vašu, ako aj domény obsahujúce phishing alebo škodlivý obsah zameraný na vašu doménu.

Ďalšiu podporu pri implementácii štandardu DMARC nájdete na **fóre DMARC** alebo v **kategórii „Chráňte svoje e-maily a povesť podniku“** na komunitnom fóre GCA.



Prepojenia „Chráňte svoje e-maily a povesť podniku“:

Súprava nástrojov: Panel nástrojov „Chráňte svoje e-maily a povesť podniku“

https://gcatoolkit.org/smallbusiness/protect-your-email-and-reputation/

Komunitné fórum: Fórum DMARC

https://community.globalcyberalliance.org/c/dmarc/5

Kategória „Chráňte svoje e-maily a povesť podniku“

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/protect-your-email-and-reputation/13

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