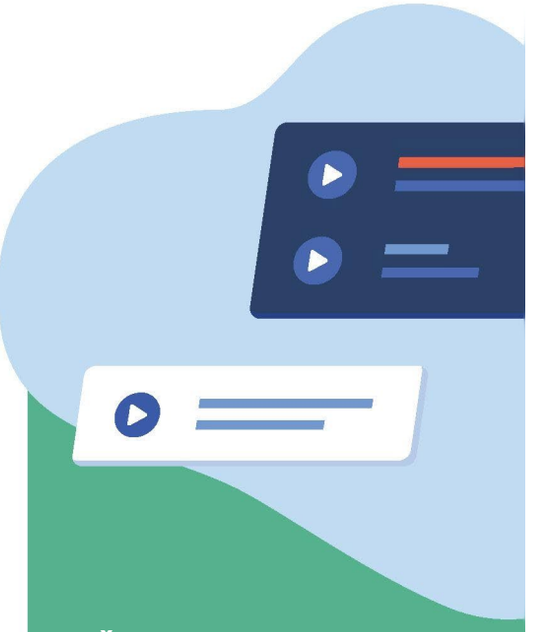
GLOBAL CYBER ALLIANCE

Príručka k súprave GCA Cybersecurity Toolkit for Small Business

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“

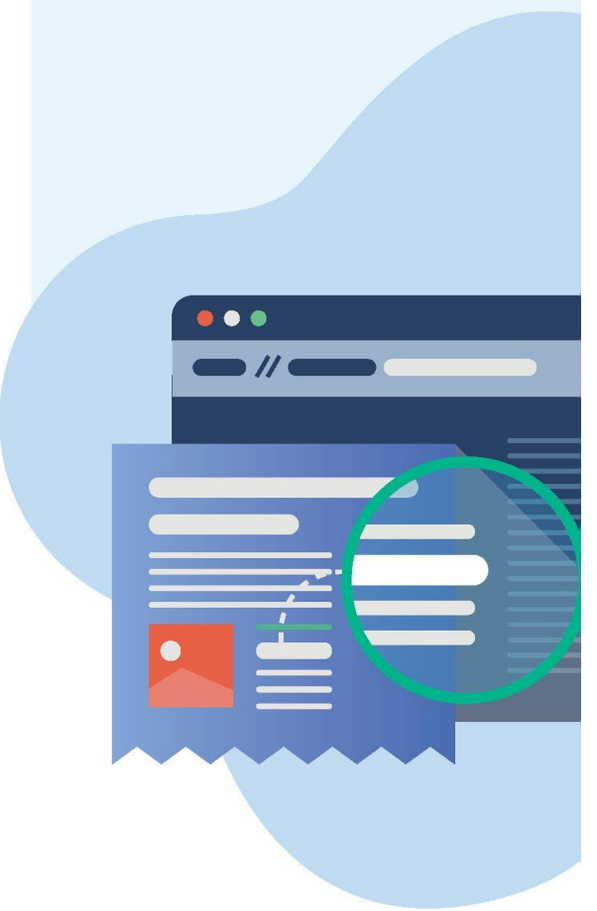
https://gcatoolkit.org/ smallbusiness/prevent-phishing- and-malware/

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



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