GCA
Cybersecurity
Toolkit™ *Para pequena empresa*

Manual do GCA Cybersecurity Toolkit para pequenas empresas

Seja bem-vindo!

Estimado(a) colega:

Atualmente, a Internet é parte integrante da atividade da maioria das empresas. Proteger o ecossistema digital da sua empresa deve fazer parte dos seus métodos de trabalho. Um ciberataque pode ter consequências devastadoras, incluindo perdas financeiras, roubo de informações confidenciais, cadeias de fornecimento comprometidas, etc.

As suas preocupações e responsabilidades são inúmeras, pelo que trabalhámos para fornecer um recurso que pode realmente utilizar para satisfazer as suas necessidades de cibersegurança. O GCA Cybersecurity Toolkit para pequenas empresas fornece ferramentas gratuitas e eficientes para reduzir o ciberrisco. As ferramentas são selecionadas e organizadas cuidadosamente para encontrar e implementar facilmente medidas importantes que irão ajudar a defender a sua empresa contra ciberameaças. Incluímos vídeos e também um fórum comunitário onde pode encontrar suporte e ver as suas perguntas respondidas pelos seus pares e especialistas em segurança. O toolkit foi criado a pensar em si e não numa pequena empresa hipotética com uma equipa de especialistas em cibersegurança e um grande orçamento.

O Manual do GCA Cybersecurity Toolkit para pequenas empresas é um complemento ao toolkit que lhe dá orientações de utilização. Pode transferir o manual na íntegra ou capítulo a capítulo, à medida que avança nas ações recomendadas no toolkit. Este guia permite-lhe trabalhar ao seu próprio ritmo para tomar medidas e irá servir de documento de referência útil para sua conveniência.

Estes recursos serão atualizados regularmente com os contributos de utilizadores, especialistas do setor e parceiros de todo o mundo.

Esperamos que tire partido do toolkit e do manual para começar a melhorar a sua cibersegurança hoje mesmo!

Atenciosamente,

Philip Reitinger
Presidente e CEO

Índice

Capítulos do manual

Conheça o seu sistema

Que problema pretende este conjunto de instrumentos abordar?

Determinar os recursos de que dispõe é o primeiro passo para melhorar a segurança, simplesmente porque não pode proteger o que não sabe que tem. Tenha em conta que muitos ciberataques e falhas de segurança dos dados ocorrem devido à perda ou ao roubo de portáteis e outros dispositivos, ao acesso não autorizado a contas e a vulnerabilidades de software sem patches. Ao determinar que computadores, dispositivos e software tem (ou seja, quais são os seus ativos), pode compreender melhor os riscos potenciais existentes, que lhe permitirão tomar decisões informadas e medidas de redução desses riscos.

- Sabe quantos portáteis e dispositivos móveis a sua empresa tem, quem tem acesso aos mesmos e que software e aplicações foram instalados?
- Sabe quantos anos têm os seus computadores e quando foi a última vez que fez uma atualização de segurança?
- Tem algum sistema ou dispositivo ligado à Internet (como câmaras de segurança ou controlo de edifícios) que também esteja ligado à rede da empresa?

Estes ativos podem abrir uma porta de acesso ao seu ambiente empresarial que permite a um hacker roubar ou danificar os seus dados. Sem sombra de dúvida que saber que dispositivos e sistemas tem é fundamental. Alguns dos seus ativos são mais importantes para as operações empresariais do que outros. Dispor de um inventário completo e atualizado ajuda a priorizar o que precisa de ser protegido e a que nível.

O que pode este conjunto de instrumentos ajudar a concretizar?

Depois de concluir este conjunto de instrumentos, compreenderá melhor:

✔ **Como realizar um inventário dos seus dados e sistemas**
✔ **Que dispositivos e aplicações são essenciais para as operações da sua empresa**

Como utilizar o conjunto de instrumentos

Utilize os instrumentos do **conjunto de instrumentos Conheça o seu sistema** para identificar mais facilmente todos os seus dispositivos (incluindo computadores, portáteis, smartphones e impressoras) e aplicações (por exemplo, e-mail, software, browsers e sites), a fim de tomar as medidas de proteção necessárias.

Este inventário servirá de guia e lista de verificações à medida que percorre os restantes conjuntos de instrumentos. Certifique-se de que mantém o inventário atualizado, incluindo sempre que adicionar ou eliminar novos equipamentos, contas ou dados essenciais.

Transfira os instrumentos do site e anote as datas de conclusão. Além disso, aproveite esta oportunidade para agendar análises regulares de forma a garantir que todas as informações estão atualizadas.

Navegar nas subcategorias do conjunto de instrumentos e informações adicionais a ter em conta

1.1 Identifique os dispositivos

Quando criar um inventário, é importante ter em conta tudo o que existe no ambiente.
Isto inclui itens como computadores, portáteis, smartphones, impressoras, CCTV, PoS, dispositivos IoT e routers.
Muitos dispositivos IoT de consumo têm poucas ou nenhumas capacidades de segurança integradas. Como tal, pondere se é possível excluí-los da rede ou removê-los por completo.

A garantia dos equipamentos mais antigos pode ter expirado, expondo-os a novas vulnerabilidades, embora sejam importantes para as operações empresariais. Estes equipamentos devem ser identificados como parte do inventário e deve ser elaborado um plano de substituição, atualização ou restrição da utilização dos mesmos.

Por vezes, muitos dispositivos, como routers, CCTV e impressoras são esquecidos quando se pensa no ambiente de TI. Contudo, tudo o que tenha uma ligação à Internet ou rede local deve ser considerado aquando da realização do inventário de ativos, uma vez que, regra geral, estas ligações constituem frequentemente uma porta que facilita o acesso à empresa.

Identifique onde os dados confidenciais e essenciais do negócio são mantidos, quer seja em dispositivos autónomos, dispositivos ligados à rede ou na cloud. É provável que estes dispositivos necessitem de níveis de proteção adicionais, mas o primeiro passo é documentar onde tudo é guardado.

1.2 Identifique as aplicações

Identifique todas as aplicações, incluindo aplicações empresariais, contas online que utilizam o seu endereço de e-mail empresarial e outras aplicações a que acede local ou remotamente através dos seus dispositivos.

É importante considerar todas as aplicações e contas, e lembrar-se de todas aquelas que já não utiliza porque são as mais suscetíveis de terem software desatualizado. Se não proporcionarem qualquer benefício, remova-as ou feche as contas. Uma conta online antiga pode conter algumas das suas informações pessoais e, se a organização para a qual configurou originalmente essa conta for alvo de uma falha de segurança, os seus dados poderão ser afetados.

Pode encontrar informações adicionais, suporte e orientação durante a implementação na **categoria Conheça o seu sistema** do Fórum Comunitário da GCA.

Ligações disponíveis em Conheça o seu sistema:

Toolkit:

Conjunto de instrumentos Conheça o seu sistema
https://gcatoolkit.org/pt-pt/pequenas-empresas/saiba-o-que-tem/

Fórum Comunitário:

Categoria Conheça o seu sistema:
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/know-what-you-have/

O fórum em outras línguas
https://community.globalcyberalliance.org/t/language-support-on-the-forum-de-es-fr-id-pt/900

Atualize as suas defesas

Que problema pretende este conjunto de instrumentos abordar?

Os cibercriminosos procuram fragilidades e falhas (conhecidas como vulnerabilidades) que podem ser utilizadas para obterem acesso a sistemas ou distribuir software malicioso. Os atores maliciosos podem obter acesso às contas financeiras da empresa, aos dados dos clientes e muito mais. Pode atualizar as suas defesas para ajudar proteger a sua empresa contra estas ameaças (ou seja, mantendo os sistemas, dispositivos e dados atualizados). Os fabricantes e os programadores de software disponibilizam regularmente atualizações de segurança para os respetivos sistemas operativos e aplicações que resolvem fragilidades ou vulnerabilidades recém-descobertas. Geralmente, estas correções são denominadas de patches e o processo de implementação é conhecido como patching.

Este conjunto de instrumentos aborda a necessidade de aplicar oportunamente estes patches, incluindo configurar sistemas, de modo a que possam ser aplicados automaticamente sempre que for possível. Além disso, é importante perceber que, ao longo do tempo, muitos sistemas são adicionados, adaptados ou reconfigurados, o que pode levar à introdução de fragilidades que podem ser exploradas pelos cibercriminosos. Outra questão a ter em mente é se um fornecedor independente tem acesso aos dados dos seus sistemas. É importante manter registos atualizados, pois permitem-lhe gerir as atualizações necessárias para garantir que os patches mais atuais são aplicados aos sistemas, aos dispositivos e às aplicações.

O que pode este conjunto de instrumentos ajudar a concretizar?

Depois de concluir este conjunto de instrumentos, compreenderá melhor como:

- ✔ Verificar se está a utilizar a versão mais recente do software no dispositivo
- ✔ Definir os dispositivos para aceitarem e aplicarem automaticamente atualizações de segurança
- ✔ Implementar definições de configuração seguras para dispositivos móveis, browsers e sistemas operativos

Como utilizar o conjunto de instrumentos

Utilize os instrumentos no **conjunto de instrumentos Atualize as suas defesas** para garantir que os seus dispositivos e as suas aplicações têm os patches de segurança mais recentes aplicados e dispõem dos níveis de segurança apropriados para o tipo de dados que contêm. Se tiver criado um inventário no conjunto de instrumentos Conheça o seu sistema, utilize este guia e lista de verificações para garantir que todos os seus dispositivos estão atualizados e definidos para aceitar automaticamente atualizações de segurança.

Depois de concluir o conjunto de instrumentos Atualize as suas defesas, atualize a lista de verificações de segurança e defina um lembrete para repetir periodicamente este processo, de modo a tornar-se uma rotina.

Navegar nas subcategorias do conjunto de instrumentos e informações adicionais a ter em conta

2.1 Atualize os dispositivos e as aplicações

Quando uma solução ou um patch é desenvolvido e lançado para uma vulnerabilidade conhecida, é importante que todos os utilizadores desse sistema ou dessa aplicação apliquem imediatamente esse patch. Idealmente de modo automático, porque até o fazerem correm risco de exposição a esta vulnerabilidade.

Verifique cada dispositivo e aplicação, e configure-os para serem atualizados automaticamente. Fornecemos uma lista dos sistemas e aplicações mais comuns, mas para aqueles não abordados neste conjunto de instrumentos, verifique as instruções ou páginas de suporte do dispositivo ou da aplicação específica. Marque cada item da lista à medida que avança e certifique-se de que segue este passo sempre que adicionar um novo dispositivo ou uma aplicação à empresa.

Muitas vezes, as configurações mais seguras não são fornecidas como predefinição de segurança pronta a utilizar (conhecida como configuração) para os dispositivos ou as aplicações, porque é dada maior prioridade à facilidade de utilização e à conveniência do que à segurança. Como tal, deve verificar se existem configurações de segurança recomendadas pelo fabricante para os dispositivos e as aplicações que possui e implementá-las.

Todos os dispositivos que deixaram de ser suportados devem ser removidos porque ficam expostos permanentemente a qualquer fragilidade recém-descoberta. Se tal não for possível, devem ser isolados de outros dispositivos e a respetiva utilização restringida a funções empresariais específicas.

Os instrumentos existentes neste conjunto de instrumentos oferecem orientações de configuração para os sistemas comuns aplicarem automaticamente as atualizações. Deve verificar as orientações para todos os seus dispositivos e sistemas de modo a garantir que são configurados em conformidade.

2.2 Encripte os dados

Se a sua rede de computadores for alvo de uma falha de segurança, muito provavelmente o *hacker* pretende roubar informações confidenciais que pode utilizar para proveito financeiro ou político próprio. A encriptação dos dados guardados no disco rígido dificulta muito mais a utilização desses dados pelos criminosos, uma vez que precisam de ser desencriptados para se tornarem utilizáveis.

A encriptação é o processo em que os dados são convertidos de um formato legível (ou seja, texto não encriptado) para um formato codificado (ou seja, texto cifrado). Esta codificação é concebida para ser incompreensível, exceto para quem possua as "chaves" para reverter o processo de codificação. A encriptação permite o armazenamento confidencial e a transmissão de dados, bem como comprovar a entidade do respetivo remetente.

Estas ferramentas permitem encriptar ficheiros guardados no disco rígido. Se o seu sistema operativo não estiver incluído neste conjunto de instrumentos, podem existir outras opções disponibilizadas pelo fabricante do equipamento ou outras ofertas de segurança à venda no mercado.

2.3 Proteja os seus sites

Para muitas empresas, o site é fundamental para as operações empresariais. O modo como é utilizado pode incluir o fluxo de informações confidenciais de toda a cadeia de abastecimento ou constituir a plataforma de negociação principal que sustenta o seu negócio. Se os *hackers* obtiverem acesso ao site, podem intercetar ou roubar dados, alterar o conteúdo, infetar o site com software malicioso ou assumir o controlo das operações. Qualquer uma destas situações pode ter um impacto devastador na capacidade operacional da organização.

Aqui, encontra ferramentas que pode utilizar para efetuar verificações regulares no site (conhecidas como análises), de modo a identificar vulnerabilidades e potenciais fragilidades. Certifique-se de que todos os problemas identificados são avaliados pelo pessoal de TI e que são tomadas medidas adequadas.

As subcategorias do conjunto de instrumentos fornecem instruções e ferramentas para sistemas comummente utilizados. Para outros cenários, procure ajuda no site do fornecedor ou aconselhamento na **categoria Atualize as suas defesas do Fórum Comunitário da GCA** ou na **Comunidade de pequenas empresas**.

Ligações disponíveis em Atualize as suas defesas:

Toolkit:

Conjunto de instrumentos Atualize as suas defesas
https://gcatoolkit.org/smallbusiness/update-your-defenses/

Fórum Comunitário:

Categoria Atualize as suas defesas
https://gcatoolkit.org/pt-pt/pequenas-empresas/atualize-as-suas-defesas/

Comunidade de pequenas empresas
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Muito mais do que simples palavras-passe

Que problema pretende este conjunto de instrumentos abordar?

As palavras-passe são a primeira linha de defesa na proteção de contas e dados (como e-mail, registos de pessoal ou bases de dados de clientes).

Infelizmente, as palavras-passe são frequentemente um alvo fácil para os cibercriminosos, e as violações de dados relacionadas com acessos ilícitos ocorrem na maior parte dos casos devido a palavras-passe fracas. Os *hackers* têm muitas maneiras de experimentar e aceder às palavras-passe, desde a utilização de decifradores de palavras-passe, que são programas que percorrem combinações comummente utilizadas facilmente obteníveis, à utilização de um nome de utilizador e de uma palavra-passe obtidos através de uma conta que foi alvo de uma falha de segurança, aplicando-as noutros sites populares. Estas técnicas precisam de poucos conhecimentos técnicos, são rápidas, totalmente automatizadas e estão imediatamente disponíveis para quem sabe onde pode encontrá-las na Internet. O problema torna-se ainda mais grave para as pequenas e médias empresas, uma vez que muitas não têm uma política de palavra-passe ou, quando existente, não a aplicam rigorosamente.

Como tal, ter palavras-passe fortes é vital para a proteção dos dados. Contudo, também é necessário outro passo como a implementação da autenticação de dois fatores ou multifator (2FA).

A 2FA requer várias credenciais, dificultando muito mais o acesso às suas contas, em caso de ataque. Com a 2FA, um utilizador necessita de:

- Algo que conhece, como uma palavra-passe;
- Algo que possui, como um token (Google Authenticator, Authy, Okta, RSA, etc.) ou um código de verificação enviado para o telemóvel;
- Ou algo físico, como a impressão digital ou o rosto (biometria).

Este conjunto de instrumentos ajuda a criar palavras-passe mais fortes e exclusivas para cada uma das suas contas, e mostra-lhe como configurar a 2FA, ambos passos importantes para proteger o acesso às contas e aos dados de que dispõe.

O que pode este conjunto de instrumentos ajudar a concretizar?

Depois de concluir este conjunto de instrumentos, compreenderá melhor como:

✔ Criar uma palavra-passe forte
✔ Testar as contas para determinar se foram comprometidas
✔ Configurar a 2FA para as contas online mais comuns

Como utilizar o conjunto de instrumentos

Utilize os instrumentos no **conjunto de instrumentos Muito mais do que simples palavras-passe** para garantir que os dispositivos e aplicações de que dispõe são configurados com palavras-passe fortes e a 2FA. Se criou um inventário em Conheça o seu sistema, utilize-o como um guia e uma lista de verificações para garantir que aplicou estas medidas em todas as suas contas.

Depois de concluir o conjunto de instrumentos Mais do que simples palavras-passe, atualize a sua lista de verificações de segurança e defina um lembrete para repetir periodicamente este processo, de modo a tornar-se uma rotina.

Navegar nas subcategorias do conjunto de instrumentos e informações adicionais a considerar

3.1 Palavras-passe fortes

Um dos métodos mais comuns que os criminosos utilizam para obter acesso a contas, redes e informações é iniciarem sessão com as suas credenciais. É realmente importante que:

- Utilize uma palavra-passe forte e única (ou frase de acesso) para cada uma das suas contas.
- Utilize letras, números e carateres especiais para garantir a criação de uma palavra-passe forte.
- Altere de imediato a palavra-passe caso seja alvo de uma falha de segurança.
- Mantenha as suas palavras-passe privadas e seguras.

- Nunca reutilize uma palavra-passe.
- Nunca clique numa ligação a pedir-lhe para repor a palavra-passe. Aceda sempre ao site da conta através do browser.
- Evite iniciar sessão em contas através de redes de Wi-Fi públicas.

Utilizar a mesma palavra-passe em várias contas significa que, se um criminoso obtiver uma das suas palavras-passe, obterá efetivamente acesso a todas as suas contas que a utilizam. Os detalhes do nome de utilizador e da palavra-passe podem ser vendidos online por criminosos que os roubaram num ciberataque e serem reutilizados até que a palavra-passe seja alterada. O rápido avanço da tecnologia significa que um portátil moderno e pouco dispendioso pode percorrer rapidamente todas as combinações para descobrir palavras-passe curtas e simples.

Deve ter uma política de palavra-passe que seja compreendida e seguida por todos os colaboradores e quaisquer adjudicatários que tenham acesso aos seus sistemas. Alguns sistemas e aplicações podem possibilitar a aplicação de uma palavra-passe mínima permitida. É certamente algo que merece ser investigado nas definições de segurança.

Pode utilizar as ferramentas disponíveis em Palavras-passe fortes para saber mais sobre palavras-passe e verificar se o seu endereço de e-mail foi roubado durante uma falha de segurança. Em caso afirmativo, altere imediatamente a palavra-passe e nunca reutilize palavras-passe.

Lembre-se também de verificar as definições de palavra-passe em routers, impressoras e outros equipamentos ligados à rede. Estes podem ser facilmente esquecidos e, geralmente, são enviados com palavras-passe predefinidas simples. Trabalhe com o inventário que criou em Conheça o seu sistema e marque os itens à medida que avança!

3.2 Ferramentas de 2FA

Além das palavras-passe, a autenticação de dois fatores (2FA) constitui uma importante segunda linha de defesa para proteger as contas contra acesso não autorizado. Existem vários métodos de autenticação diferentes que podem ser utilizados como 2FA. Estes incluem um código único enviado por SMS para o telemóvel, um token de hardware que transporte sempre consigo, uma impressão digital ou o reconhecimento facial.

As ferramentas de 2FA contém recursos transferíveis que fornecem métodos de autenticação aceites para muitas contas comuns.

Quando implementar os instrumentos e as orientações do conjunto de instrumentos Muito mais do que simples palavras-passe, considere também quais são as permissões cada utilizador tem quando acede a aplicações empresariais. Considere restringir o acesso apenas aos utilizadores que precisam dele e na medida em que a respetiva função o exija.

3.3 Faça a gestão das suas palavras-passe

Os gestores de palavras-passe permitem manter todas as suas palavras-passe num local seguro para não ter de se lembrar de cada uma individualmente. Isto significa que só tem de se lembrar de uma palavra-passe sempre que quiser iniciar sessão numa das contas cuja palavra-passe está guardada no

gestor de palavras-passe. Os gestores de palavras-passe são efetivamente práticos. No entanto, se o gestor de palavras-passe for comprometido, o atacante pode obter acesso a todas as palavras-passe.

Pode encontrar informações adicionais, suporte e orientação durante a implementação na **categoria Muito mais do que simples palavras-passe** ou no Fórum Comunitário da GCA.

Ligações disponíveis em Muito mais do que simples palavras-passe:

Toolkit:

Conjunto de instrumentos Muito Mais do que Simples Palavras-passe
https://gcatoolkit.org/pt-pt/pequenas-empresas/muito-mais-do-que-simples-palavras-passe/

Fórum Comunitário:

Categoria Muito Mais do que Simples Palavras-passe
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/beyond-simple-passwords/

Impeça o phishing e o malware

Que problema pretende este conjunto de instrumentos abordar?

Todos os anos, muitas pequenas empresas são vítimas de ataques dispendiosos de software malicioso e phishing. Quando um utilizador clica num site infetado com software malicioso ou abre um anexo infetado num e-mail de phishing, podem ocorrer vários problemas como a eliminação ou alteração dos ficheiros, a modificação de aplicações ou a desativação das funções do sistema.

Software malicioso é qualquer software concebido para causar danos e/ou permitir o acesso não autorizado a dispositivos ou redes. Os e-mails de phishing levam o utilizador a pensar que está a lidar com uma entidade fidedigna para que o atacante possa obter acesso não autorizado a conteúdo privado, sensível e restrito ou dinheiro. O atacante fará o que puder para que o respetivo e-mail pareça genuíno e atraente de modo a incentivar o utilizador a clicar nele ou a abri-lo. Os e-mails podem parecer ter um remetente que conhece, podem

imitar os logótipos e o formato dos e-mails de organizações conhecidas, podem referir-se a notícias recentes ou a um trabalho que acabou de fazer.

Algumas estimativas sugerem que mais de 90% dos ciberataques começam com um e-mail de phishing. Se clicar no link ou abrir o anexo num e-mail de phishing, poderá acionar inúmeras atividades que o atacante tenha configurado, desde roubar os seus dados, criar uma rota secreta (conhecida como backdoor) no seu computador para utilização posterior, instalar um tipo de software malicioso através do qual bloqueia o acesso aos dados e exigir que lhe pague um resgate para recuperar o acesso (conhecido como ransomware) ou transferir outro tipo de software malicioso que permita ver o que escreve, como palavras-passe ou números de conta (conhecido como spyware).

As consequências dos ataques de phishing e software malicioso são graves para as pequenas empresas. Os efeitos podem incluir perda ou danos nos dados, perda de receitas, se a empresa tiver de encerrar durante um ataque, despesas incorridas para reparar/substituir equipamentos, custos para notificar os clientes sobre uma falha de segurança e ainda perda de reputação e possíveis processos legais.

O que pode este conjunto de instrumentos ajudar a concretizar?

O **conjunto de instrumentos Evite phishing e software malicioso** aumenta a resiliência a ataques para ajudar a reduzir os riscos. Foram incluídas ferramentas para ajudar a impedir o acesso a sites infetados, software antivírus para ajudar a impedir vírus e outro software malicioso de entrarem nos sistemas e bloqueadores de publicidade para ajudar a bloquear anúncios online que podem transportar vírus.

Depois de concluir este conjunto de instrumentos, compreenderá melhor:

- ✔ De que forma o software antivírus protege os sistemas e os dados
- ✔ Como instalar software antivírus no sistema
- ✔ O que são anúncios digitais e os riscos inerentes
- ✔ Como instalar um bloqueador de publicidade para bloquear anúncios pop-up, vídeos e outro conteúdo indesejado
- ✔ O que significa DNS e por que razão é importante
- ✔ Como funciona a segurança DNS e que tipos de ataques mitiga
- ✔ Como instalar o Quad9 em dispositivos Android e computadores

Navegar nas subcategorias do conjunto de instrumentos e informações adicionais a ter em conta

As ferramentas foram cuidadosamente escolhidas com base em normas globais reconhecidas e não são apresentadas aqui numa ordem específica nem prioridade recomendada.

4.1. Antivírus

É importante utilizar sistemas de antivírus em tempo real porque estes procuram vírus em tempo real no preciso momento em que ocorrem, removendo-os antes de poderem causar danos, e são atualizados à medida que novas proteções contra vírus são desenvolvidas.

4.2 Bloqueadores de publicidade

Alguns anúncios online ou mensagens apresentadas enquanto navega num site são úteis. No entanto, outros podem conter código malicioso e infetar o computador com software malicioso se clicar neles. Um bloqueador de publicidade pode ser utilizado para impedir a apresentação de anúncios em páginas Web, oferecendo proteção adicional durante a navegação.

4.3 Segurança DNS

A segurança DNS utiliza o Sistema de Nomes de Domínio (o equivalente na Internet a uma lista telefónica) para traduzir o nome do site baseado em texto (nome de domínio) que um utilizador escreve no browser para um conjunto de números (endereço IP) único que os computadores compreendem.

Muitos atacantes tentam utilizar nomes de domínio de sites semelhantes para levar as vítimas a pensar que estão a ligar-se a um site legítimo. Estes sites podem parecer ter o nome real do site, mas uma inspeção mais atenta pode mostrar as diferenças.

Assim, por exemplo, o URL do site legítimo de uma empresa pode ser: "www. mygreatwidgets. com", mas o falso pode ser: "www. rnygreatwidgets. com".

As firewalls DNS, um tipo de segurança DNS, podem ajudar a impedir vírus e ataques de phishing porque verificam se o endereço IP do site que está a ser pedido é conhecido por alojar código malicioso e, se for o caso, bloqueiam o acesso. Os utilizadores podem implementar serviços de filtragem de DNS nos respetivos sistemas através das ferramentas desta subcategoria para ajudar a impedir o acesso a sites maliciosos conhecidos.

As subcategorias do conjunto de instrumentos fornecem ferramentas para sistemas comummente utilizados. Para obter mais suporte, pesquise ou faça perguntas no Fórum Comunitário da GCA **Evite phishing e software malicioso** ou na **Comunidade de pequenas empresas**.

Ligações disponíveis em Evite phishing e software malicioso:

Toolkit:

Toolkit Evite phishing e software malicioso
https://gcatoolkit.org/pt-pt/pequenas-empresas/evite-phishing-e-software-malicioso/

Fórum Comunitário:

Categoria Evite phishing e software malicioso
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/prevent-phishing-and-viruses/

Comunidade de pequenas empresas
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Cópias de segurança e recuperação

Que problema pretende este conjunto de instrumentos abordar?

A perda ou corrupção de dados pode resultar de ciberataques (como ransomware), falhas ou roubos de equipamento, erro humano, danos acidentais, incêndio ou inundação. Independentemente da causa, o impacto da perda de dados ou do tempo de inatividade do equipamento pode afetar seriamente a produtividade e a rentabilidade da sua empresa.

Uma cópia de segurança é uma cópia dos dados, guardada num local diferente do local dos dados originais, e pode ajudar a recuperar de um ataque ou de uma perda de dados. A realização regular de cópias de segurança online e offline facilita uma recuperação mais rápida da perda ou corrupção dos dados. Ambas são importantes porque as cópias de segurança online são configuradas para serem realizadas automaticamente numa rede, enquanto as cópias de segurança offline exigem a ligação e posterior remoção de um dispositivo externo (por exemplo, uma pen USB ou um disco rígido) para armazenamento físico noutro local (o que também ajuda a proteger contra a cópia de segurança acidental de dados já corrompidos).

O que pode este conjunto de instrumentos ajudar a concretizar?

Depois de concluir este conjunto de instrumentos, compreenderá melhor:

- ✔ Por que razão as cópias de segurança são importantes para a sua empresa, em especial para a recuperação de um ataque de ransomware
- ✔ Como ativar a cópia de segurança integral num computador Windows ou Mac

Como utilizar o conjunto de instrumentos

Utilize os instrumentos no **conjunto de instrumentos Cópias de segurança e recuperação** para garantir a realização regular de cópias de segurança dos sistemas com um nível e uma frequência adequados para o tipo de dados que contêm.

O que deve incluir nas cópias de segurança? Depende das suas informações e do risco de perda dessas informações. Se criou um inventário no conjunto de instrumentos Conheça o seu sistema, utilize-o como um guia e uma lista de verificação, e atualize-o à medida que avança.

Depois de concluir o conjunto de instrumentos Cópias de segurança e recuperação, atualize a lista de verificações de segurança e defina um lembrete de revisão periódica para garantir que a sua política permanece relevante para a sua empresa.

Navegar nas subcategorias do conjunto de instrumentos e informações adicionais a ter em conta

O ransomware é um método de ataque que se tornou um problema sério para as pequenas empresas. Consiste num tipo de software malicioso que infeta computadores e bloqueia o acesso aos dados. O criminoso exige pagamento, por vezes na forma de criptomoeda (ou seja, bitcoin, que é menos fácil de rastrear do que as transferências tradicionais), com a promessa de que os dados serão restaurados assim que o resgate for recebido. Manter cópias de segurança dos dados é uma proteção importante para manter o acesso às suas informações, se for vítima de ransomware.

5.1 Cópia de segurança de sistemas operativos

Ter uma política sólida de cópia de segurança que inclua cópias de segurança online e offline ajuda a facilitar uma recuperação mais rápida em caso de perda ou corrupção dos dados.

- Os diferentes conjuntos de dados que possui devem ser categorizados no inventário (consulte o conjunto de instrumentos Conheça o seu sistema para obter ajuda para a criação de um inventário).
- Considere encriptar as informações confidenciais (consulte o conjunto de instrumentos Atualize as suas defesas para obter mais informações sobre a encriptação).
- Ponha em prática uma abordagem lógica de cópia de segurança de cada conjunto de dados após ter ponderado o "impacto da perda" de cada um. O impacto da perda pode ser reputacional, financeiro ou legal.

Na subcategoria Cópia de segurança de sistemas operativos, encontra instruções para a realização de cópias de segurança de sistemas operativos comuns. Se o seu sistema operativo não constar da lista, procure ajuda no site do fornecedor ou pesquise na **categoria Cópias de segurança e recuperação** do Fórum Comunitário da GCA.

Certifique-se também de que tem um plano de recuperação em caso de catástrofe, o que ajuda a permitir a recuperação de sistemas essenciais após uma catástrofe (acidental ou natural). Ter um plano ajuda a minimizar o tempo de recuperação e os danos nos sistemas, protege contra possíveis responsabilidades e também pode melhorar a segurança. Existem muitos modelos e guias para o desenvolvimento de um plano disponíveis online. Certifique-se de que mantém o plano atualizado e simule alguns cenários para o testar e garantir que todos sabem como implementá-lo.

Ligações disponíveis em Cópias de segurança e recuperação:

Toolkit:

Conjunto de instrumentos Cópias de segurança e recuperação
https://gcatoolkit.org/pt-pt/pequenas-empresas/copia-de-seguranca-e-recuperacao/

Fórum Comunitário:

Cópias de segurança e recuperação
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/back-up-and-recover/

Proteja o seu e-mail e a sua reputação

Que problema pretende este conjunto de instrumentos abordar?

O e-mail é utilizado frequentemente como ponto de partida para um ciberataque. É extremamente rápido e pouco dispendioso enviar milhares de e-mails para destinatários incautos na esperança de que, pelo menos, alguns utilizadores sejam levados a clicar na ligação do site malicioso ou transferir o anexo nocivo.

Uma das técnicas que os cibercriminosos utilizam é fazer com que o e-mail pareça ter sido enviado a partir de uma origem legítima, como uma instituição financeira, um cliente, um parceiro de negócios ou outra organização familiar. Uma dessas técnicas é conhecida como spoofing (usurpação) do domínio de e-mail, em que o endereço de e-mail "spoofed" (usurpado) utilizado é exatamente igual ao

genuíno, fazendo com que pareça ter sido efetivamente enviado por essa organização e dando ao destinatário poucos motivos para suspeitar do contrário.

Se o domínio de e-mail da sua empresa (a parte do endereço de e-mail após a "@") for usurpado, pode ter graves consequências para si, para os seus clientes e para a cadeia de abastecimento. Se o destinatário desse e-mail agiu como sugerido no e-mail porque realmente acreditava que tinha sido enviado por si, o respetivo sistema informático pode ser infetado com algum tipo de software malicioso ou ransomware. Também pode permitir que o criminoso assuma o controlo e manipule os seus dados bancários, para que os clientes façam pagamentos para outras contas pensando que lhe estão a pagar.

O conjunto de instrumentos Proteja o seu e-mail e a sua reputação fornece orientação e ferramentas para se proteger contra este tipo de ameaça, inclusive instruções de utilização de um padrão de correio eletrónico conhecido como DMARC (Domain-based Authentication, Reporting, and Conformance). O DMARC é uma maneira eficiente de impedir os remetentes de spam e phishers de utilizarem domínios de empresas para levarem a cabo ciberataques perigosos. É uma forma de verificar se o remetente de um e-mail tem permissão para utilizar o domínio do seu e-mail e enviar mensagens.

Os atacantes também podem configurar sites "sósia". Por exemplo, o domínio genuíno "BestBusiness .com" pode ser usurpado mediante o registo como "BestBusness .com" ou "BestBusiness .net" para levar os clientes ou utilizadores a visitá-lo.

Se os domínios do e-mail ou site forem usurpados, a sua reputação e marca podem ser afetadas, e os seus clientes prejudicados. Utilizar os instrumentos do conjunto Proteja o seu e-mail e a sua reputação ajuda a identificar e evitar a usurpação de identidade.

O que pode este conjunto de instrumentos ajudar a concretizar?

Depois de concluir este conjunto de instrumentos, compreenderá melhor:

- ✔ O que significa DMARC, por que razão é importante e que ataques mitiga
- ✔ O guia de configuração do DMARC
- ✔ Como verificar o seu próprio domínio de e-mail para ver se o DMARC está ativado

Como utilizar o conjunto de instrumentos

Utilize os instrumentos do **conjunto de instrumentos Proteja o seu email e a sua reputação** para garantir que a sua empresa está protegida contra spoofing de domínio de e-mail através da implementação do DMARC e identificar potenciais domínios de sites fraudulentos.
Atualize a sua lista de verificações de segurança quando concluir e incentive os seus clientes e a cadeia de abastecimento com domínios próprios a fazerem o mesmo, uma vez que a eficiência do DMARC depende de tanto o remetente como o destinatário terem implementado este mesmo padrão.

Navegar nas subcategorias do conjunto de instrumentos e informações adicionais a ter em conta

6.1 Implementar o DMARC

Utilize os instrumentos nesta subcategoria para saber mais sobre o DMARC, verificar se o seu domínio de e-mail está protegido pelo DMARC e, em caso afirmativo, até que nível.

6.2 Compreender relatórios de DMARC

Depois de configurar uma política de DMARC no domínio de e-mail, começa a receber relatórios que mostram como o seu domínio de e-mail está a ser utilizado. Estes relatórios podem ser difíceis de compreender sem um formato definido.

Os instrumentos na subcategoria Compreender relatórios de DMARC ajudam a interpretar e identificar mais rapidamente a atividade fraudulenta. Isto permite-lhe avançar com confiança nos níveis de política de "nenhum" para "quarentena" para chegar, por fim, ao nível mais alto "rejeitar". É importante também considerar qualquer organização ou serviço de e-mail autorizado a enviar e-mails em seu nome, como serviços de marketing por e-mail, e verificar se estes implementaram o DMARC.

As vantagens do DMARC só serão visíveis quando o seu domínio de e-mail alcançar o nível "rejeitar".

6.3 Proteção de marca registada

Os autores das fraudes podem registar domínios parecidos com o seu domínio na esperança de que as pessoas cliquem neles. Utilize as ferramentas disponibilizadas aqui para simplificar a identificação de domínios que tentam imitar o seu, bem como domínios que contêm phishing ou conteúdo malicioso direcionado para o seu domínio.

Para obter mais suporte durante a implementação do DMARC, consulte o **Fórum DMARC** ou a **categoria Proteja o seu email e a sua reputação** no Fórum Comunitário da GCA.

Ligações disponíveis em Proteja o seu email e a sua reputação:

Toolkit:

Toolkit Proteja o seu email e a sua reputação
https://gcatoolkit.org/pt-pt/pequenas-empresas/proteja-o-seu-e-mail-e-a-sua-reputacao/

Fórum Comunitário:

Fórum DMARC
https://community.globalcyberalliance.org/c/dmarc/

Categoria Proteja o seu email e a sua reputação
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/protect-your-email-and-reputation

Manual do GCA Cybersecurity Toolkit para pequenas empresas

Glossário de termos

Glossário de alguns termos comummente utilizados relacionados com cibersegurança. Alguns destes termos foram incluídos nos capítulos do Manual do GCA Cybersecurity Toolkit para pequenas empresas, enquanto outros são fornecidos como informações adicionais, caso deseje explorar um pouco mais por conta própria.

conta Refere-se geralmente a um acesso a um sistema de computador ou serviço online que requer normalmente uma palavra-passe para entrar.

adversário Um indivíduo, grupo, organização ou governo que realiza ou tem a intenção de realizar atividades prejudiciais.

antivírus Software projetado para detetar, impedir e remover vírus e outros tipos de software malicioso.

aplicação (app) Um programa projetado para executar tarefas específicas. Normalmente, o termo app refere-se a programas transferidos para dispositivos móveis.

ativo Qualifica-se como pessoa, estrutura, instalação, informação, registos, sistemas e recursos de tecnologia da informação, material, processo, relações ou reputação que tenha valor. Qualquer coisa útil que contribua para o sucesso de algo, como uma missão organizacional. Os ativos são coisas de valor ou propriedades às quais é possível atribuir valor.

ataque Uma tentativa de obter acesso não autorizado a serviços, recursos ou informações do sistema, ou uma tentativa de comprometer a integridade do sistema. O ato intencional de tentar contornar um ou mais serviços de segurança ou controlos de um sistema de informação.

assinatura de ataque Um padrão característico ou distintivo que pode ser pesquisado ou utilizado na correspondência com ataques identificados anteriormente.

superfície de ataque O conjunto de formas através das quais um adversário pode aceder a um sistema e potencialmente causar danos. São também características de um sistema de informação que permitem que um adversário investigue, ataque ou mantenha a presença no sistema de informação.

atacante Ator malicioso que pretende explorar sistemas informáticos com a intenção de alterar, destruir, roubar ou desativar as respetivas informações e, em seguida, explorar o resultado.

autenticação O processo para verificar se alguém é quem afirma ser quando tenta aceder a um computador ou serviço online. Também consiste na origem e integridade dos dados, no utilizador, processo ou dispositivo.

backdoor Uma forma secreta de os cibercriminosos obterem acesso não autorizado a um sistema informático
cópia de segurança Uma cópia dos dados, guardada num local diferente do local dos dados originais, que pode ajudar a recuperar de um ataque ou de uma perda de dados.

criar cópias de segurança Fazer cópias dos dados guardados num computador ou servidor para diminuir o impacto potencial da falha ou perda.

bot Um computador ou dispositivo ligado à Internet que foi comprometido secretamente por código malicioso para realizar atividades sob o comando e o controlo de um administrador remoto.

botnet Uma rede de dispositivos infetados (bots) ligados à Internet, utilizados na realização de ciberataques coordenados sem o conhecimento do proprietário.

violação Um incidente no qual dados, sistemas informáticos ou redes são acedidos ou afetados de forma não autorizada.

ataque de força bruta Utilizar um poder computacional para inserir automaticamente um grande número de combinações de valores, geralmente para descobrir palavras-passe e obter acesso.

erro Defeito, falha, deficiência ou imperfeição inesperada e relativamente pequena num sistema de informação ou dispositivo.

configuração A disposição dos componentes de software e hardware de um sistema informático ou dispositivo.

configurar O processo de configurar o software ou dispositivos para um computador, sistema ou tarefa específica.

ciberataque Tentativas maliciosas de danificar, interromper ou obter acesso não autorizado a sistemas informáticos, redes ou dispositivos através de meios cibernéticos.

ciberincidente Uma falha nas regras de segurança para um sistema ou serviço. Mais comummente, tentativas de obter acesso não autorizado a um sistema e/ou dados, utilização não autorizada de sistemas para o processamento ou armazenamento de dados, alterações no firmware, software ou hardware de sistemas sem o consentimento dos respetivos proprietários, interrupção maliciosa e/ou negação de serviço.

cibersegurança A proteção de dispositivos, serviços e redes, e as respetivas informações, contra roubo ou danos.

criptomoeda Dinheiro digital. A criptomoeda é guardada numa carteira digital (online, no computador ou noutro hardware.) Normalmente, a criptomoeda não tem aval de nenhum governo e, como tal, não tem as mesmas proteções que o dinheiro existente num banco.

ataque por dicionário Um tipo de *ataque de força bruta* no qual o atacante utiliza palavras do dicionário, frases ou palavras-passe comuns conhecidas como suposições.
pegada digital Uma "pegada" de informações digitais que a atividade online de um utilizador deixa para trás.

negação de serviço (DoS) Um ataque no qual o acesso aos serviços do computador (ou recursos) é negado aos utilizadores legítimos, geralmente sobrecarregando o serviço com pedidos.

dispositivo Uma peça de hardware informático projetada para uma função específica. São exemplos disso portáteis, telemóveis ou impressoras.

DMARC Significa Domain-based Message Authentication, Reporting and Conformance. DMARC é um mecanismo que permite que os remetentes e destinatários monitorizem e melhorem a proteção do respetivo domínio contra e-mails fraudulentos.

spoofing de domínio de e-mail Uma técnica utilizada por cibercriminosos na qual o endereço de e-mail usurpado ("spoofed") utilizado é exatamente igual ao genuíno, fazendo com que pareça ter sido efetivamente enviado por essa organização.

encriptação Conversão de dados num formato que não pode ser facilmente compreendido por pessoas não autorizadas.

firewall Um dispositivo de hardware/software ou um programa de software que limita o tráfego de rede de acordo com um conjunto de regras que estipulam que acesso é ou não permitido ou autorizado.

hacker Alguém que viola a segurança do computador por razões maliciosas, elogios ou ganho pessoal.

hardware Um computador, os respetivos componentes e equipamento relacionado. O hardware inclui unidades de disco, circuitos integrados, monitores, cabos, modems, altifalantes e impressoras.

ameaça interna Uma pessoa ou um grupo de pessoas com acesso e/ou conhecimento interno de uma empresa, organização ou firma que pode representar um risco potencial por violar políticas de segurança com a intenção de causar danos.

Internet das coisas (IoT) Refere-se à capacidade de objetos de utilização quotidiana (em vez de computadores e dispositivos) se ligarem à Internet. Exemplos incluem chaleiras, frigoríficos e televisores.

intrusão Um ato não autorizado de contornar os mecanismos de segurança de uma rede ou de um sistema de informação.

sistema de deteção de intrusão (IDS) Programa ou dispositivo utilizado para detetar se um atacante está ou tentou aceder sem autorização aos recursos do computador.

sistema de prevenção de intrusão (IPS) Sistema de deteção de intrusão que também bloqueia o acesso não autorizado quando é detetado.

registador de teclado Software ou hardware que rastreia batimentos de tecla e eventos de teclado, em geral secretamente, para monitorizar ações do utilizador de um sistema de informação.

publicidade mal-intencionada Utilizar publicidade online como método de entrega de malware.

software malicioso (malware) Uma expressão que inclui vírus, cavalos de troia, worms ou qualquer código ou conteúdo que possa ter um impacto adverso em organizações ou indivíduos. Software destinado a infiltrar-se e danificar ou desativar computadores.

mitigação A aplicação de uma ou mais medidas para reduzir a probabilidade de uma ocorrência indesejada e/ou de atenuar as respetivas consequências.

rede Dois ou mais computadores ligados tendo em vista a partilha de recursos.

ameaça externa Uma pessoa ou um grupo de pessoas não pertencentes a uma organização que não estão autorizadas a aceder aos respetivos ativos e representam um risco potencial para a organização e respetivos ativos.

palavra-passe Uma cadeia de carateres (letras, números e outros símbolos) utilizada para autenticar uma identidade ou verificar a autorização de acesso.

decifradores de palavras-passe Programas concebidos para adivinhar uma palavra-passe, muitas vezes passando por combinações comummente utilizadas ou um nome de utilizador e uma palavra-passe obtidos a partir de uma conta alvo de uma falha de segurança.

gestores de palavras-passe Programas que permitem aos utilizadores gerar, guardar e gerir palavras-passe numa localização, de forma segura.

aplicação de patches Aplicar atualizações ao firmware ou software para melhorar a segurança e/ou a funcionalidade.

teste de penetração (pentest) Um teste autorizado a uma rede ou um sistema informático concebido para procurar fragilidades de segurança para que possam ser corrigidas.

elementos de identificação/informações sobre a identificação (PII) As informações que permitem que a identidade de um indivíduo seja direta ou indiretamente inferida.

pharming Um ataque à infraestrutura de rede que resulta no direcionamento do utilizador para um site ilegítimo, apesar de o utilizador ter inserido o endereço correto.

phishing E-mails em massa não direcionados, enviados para muitas pessoas a pedir informações confidenciais (como dados bancários) ou incentivando-as a visitar um site falso. Uma forma digital de engenharia social para levar os indivíduos a fornecer informações confidenciais.
texto simples Informações não encriptadas.

servidor proxy Servidor que atua como intermediário entre os utilizadores e outros servidores, validando os pedidos dos utilizadores.

ransomware Software malicioso que torna os dados ou os sistemas inutilizáveis até a vítima efetuar um pagamento.

recuperação As atividades após um incidente ou evento para restaurar serviços e operações essenciais a curto e médio prazo, e restaurar totalmente todos os recursos a longo prazo.

resiliência A capacidade de adaptação às condições em mudança e preparação, resistência e recuperação rápida da interrupção.

restaurar A recuperação de dados após falha ou perda do computador.

avaliação de riscos O processo de identificação, análise e avaliação de riscos, juntamente com as potenciais consequências nocivas, com o objetivo de informar prioridades, desenvolver ou comparar cursos de ação e fundamentar a tomada de decisões.

Gestão de Informações e Eventos de Segurança (SIEM) Processo no qual as informações de rede são agregadas, ordenadas e correlacionadas para a deteção de atividades suspeitas.

smishing Phishing via SMS: mensagens de texto em massa enviadas aos utilizadores a pedir informações confidenciais (por exemplo, detalhes bancários) ou incentivando-os a visitar um site falso.

assinatura Um padrão distintivo reconhecível. Os tipos de assinaturas podem incluir assinatura de ataque, assinatura digital e assinatura eletrónica.

engenharia social Manipular pessoas para realizarem ações específicas ou divulgarem informações que são úteis para um atacante.

software Refere-se a programas para controlar o funcionamento de um computador ou processar dados eletrónicos.

spam O abuso de sistemas de mensagens eletrónicas para enviar indiscriminadamente mensagens em massa não solicitadas.

ciberiscagem personalizada Uma forma mais direcionada de phishing em que o e-mail é projetado para parecer que é de uma entidade que o destinatário conhece e/ou em quem confia.

spoofing Falsificação do endereço de envio de uma transmissão para obter acesso ilegal [não autorizado] a um sistema seguro. A usurpação de identidade, a dissimulação, o piggybacking e a imitação são formas de spoofing.
spyware Software malicioso que transmite informações sobre as atividades do utilizador de um computador a uma entidade externa.

cadeia de abastecimento Um sistema de organizações, pessoas, atividades, informações e recursos que cria e move produtos, incluindo componentes de produtos e/ou serviços de fornecedores para os respetivos clientes.

sistema Geralmente, refere-se a um sistema de um ou mais computadores ou dispositivos que introduzem, enviam, processam e armazenam dados e informações.

administrador de sistema (admin) Pessoa que instala, configura, resolve problemas e mantém as configurações do servidor (hardware e software) para garantir a respetiva confidencialidade, integridade e disponibilidade. Também gere contas, firewalls e patches e é responsável pelo controlo do acesso, palavras-passe, criação de contas e administração.

ameaça Algo que possa causar danos num sistema ou numa organização.

ator da ameaça Um indivíduo, grupo, organização ou governo que realiza ou tem a intenção de realizar atividades nocivas.

cavalo de troia Um programa informático que é disfarçado de software legítimo, mas com uma função oculta utilizada para invadir o computador da vítima. Um tipo de software malicioso.

autenticação de dois fatores (2FA) A utilização de dois componentes diferentes para verificar a identidade afirmada de um utilizador. Também conhecida como autenticação multifator.

rede virtual privada (VPN) Uma rede encriptada frequentemente criada para permitir ligações seguras para utilizadores remotos; por exemplo, numa organização com escritórios em vários locais.

vírus Um programa informático que pode replicar-se, infetar um computador sem permissão ou conhecimento do utilizador e, em seguida, espalhar-se ou propagar-se para outro computador. Um tipo de software malicioso

vulnerabilidade Uma fragilidade, ou falha, no software, num sistema ou num processo. Um atacante pode tentar explorar uma vulnerabilidade para obter acesso não autorizado a um sistema.

ciberiscagem de peixe graúdo Ataques de phishing altamente direcionados (mascarados de e-mails legítimos) que visam executivos seniores.

worm Um programa autorreplicante, autopropagante e autocontido que utiliza mecanismos de rede para se propagar. Um tipo de software malicioso

Definições compiladas a partir de recursos produzidos pelas seguintes entidades:

British Standards Institute
https://www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

National Cyber Security Centre (NCSC-UK)
https://www.ncsc.gov.uk/information/ncsc-glossary

National Initiative for Cybersecurity Careers and Studies (NICCS-US)
https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

Recursos adicionais:

Glossário do Australian Cyber Security Centre
https://www.cyber.gov.au/acsc/view-all-content/glossary

Global Knowledge
https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/

Glossário de termos de segurança do SANS Institute
https://www.sans.org/security-resources/glossary-of-terms/