Acompanhamento de Segurança Cibernética

Contextualização

O Tribunal de Contas da União (TCU) publicou, recentemente, sua "Estratégia de Fiscalização em Segurança da Informação e Segurança Cibernética 2020-2023", no âmbito da qual é prevista a realização desta fiscalização, do tipo "acompanhamento", com vistas a obter dados e avaliar a adoção, pelas organizações públicas federais, de controles críticos para a gestão de segurança cibernética (SegCiber).

O método utilizado é o de autoavaliação de controles internos (do inglês *Control Self-Assessment* – CSA), no qual disponibiliza-se um questionário para que o gestor preencha as respostas que melhor reflitam a situação atual da sua organização com relação aos controles e medidas de segurança questionados. Além de fornecer à organização um diagnóstico do seu grau de maturidade atual com relação a tais controles e medidas de segurança, essa metodologia permite que os gestores e a unidade de auditoria interna continuem avaliando a organização mesmo após o término da fiscalização e, assim, possam conduzir por conta própria seu aumento de maturidade ao longo dos próximos anos, com a implantação dos controles internos necessários.

Recomenda-se que o respondente possua perfil técnico e, idealmente, seja o gestor ou esteja lotado em unidade responsável pela gestão da segurança de tecnologia da informação (TI) da organização. A título orientativo, esclarece-se que os critérios utilizados para subsidiar a elaboração deste questionário foram livremente adaptados a partir do julgamento profissional da equipe de auditores do TCU sobre a versão 8 do *framework* desenvolvido pelo *Center for Internet Security* (CIS). Dos dezoito controles críticos de SegCiber listados nessa versão, o questionário abordará os seguintes:

1) Inventário e controle de ativos corporativos

2) Inventário e controle de ativos de software

7) Gestão contínua de vulnerabilidades

14) Conscientização sobre segurança e treinamento de competências

17) Gestão de respostas a incidentes

Cada um desses controles é subdividido em medidas de segurança, isto é, ações específicas que a organização precisa executar de modo a implementar efetivamente aquele controle. Cada medida de segurança, a seu turno, é subdividida em um conjunto de subpráticas que se somam para materializá-la.

Este código de acesso (token:) corresponde às respostas da organização: .

Observações importantes:

1) O texto do questionário foi previamente validado com o intuito de minimizar dúvidas de interpretação em relação às perguntas e às possibilidades de resposta correspondentes. Aconselha-se que o questionário seja preenchido assim que recebido, frisando-se que eventuais solicitações de esclarecimentos (a serem encaminhadas para o e-mail segciber@tcu.gov.br) podem não ser respondidas a tempo e que isso não justifica o não preenchimento completo e envio do questionário até 22/10/2021.

2) Por conterem informações relacionadas à segurança cibernética da organização, as respostas submetidas no âmbito desta fiscalização serão, de antemão, classificadas como reservadas, nos termos do art. 23, inciso VII, c/c o art. 24, § 1º, inciso III, da Lei 12.527/2011 (Lei de Acesso à Informação – LAI).

3) Com este acompanhamento, o TCU visa a diagnosticar a maturidade das organizações públicas federais em relação aos critérios questionados, ciente de que uma maturidade maior implica em custos mais elevados e que, portanto, a definição do grau de maturidade mais adequado a cada organização é, essencialmente, uma decisão de gestão (tomada com base no tipo de negócio, apetite a riscos, custo e expectativa de retorno da implementação de controles internos específicos etc.), a qual deve estar amparada por análises devidamente fundamentadas.

4) O questionário não é exaustivo quanto às medidas de segurança possíveis de serem implementadas no escopo dos controles abordados. Há questões que abrangem medidas de segurança que podem não ser aplicáveis a algumas organizações, por razões diversas (*e.g.* contexto específico, porte e objetivos institucionais).

5) Para cada medida de segurança questionada, o gestor deve responder duas perguntas. Na primeira (questões do tipo A), deve ser marcada a opção, dentre as seguintes, que melhor reflita a situação da sua organização em relação à respectiva adoção: a) "Não adota"; b) "Há decisão formal ou plano aprovado para adotá-la"; c) "Adota em menor parte"; d) "Adota parcialmente"; e) "Adota em maior parte ou totalmente"; f) "Não se aplica". No caso das respostas "d" e "e", devem ser descritas as evidências dessa adoção. No caso da resposta "f", deve ser justificado o entendimento pela não aplicação. Logo em seguida, o gestor deve marcar todas as opções de subpráticas que se encontram efetivamente implementadas na sua organização, relativamente àquela medida de segurança (questões do tipo B).

6) A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário (22/10/2021), os auditores do TCU poderão requisitar o envio das evidências referidas no item anterior (mencionadas pelo gestor para justificar sua resposta no sentido de que a organização adota parcial ou totalmente determinada medida de segurança), bem como de quaisquer outras que considerem pertinentes.

7) O respondente pode navegar à vontade entre os grupos de questões por meio dos botões "Próximo" e "Anterior" localizados no rodapé das páginas. O botão "Próximo", no entanto, só permitirá o avanço se as perguntas obrigatórias do grupo/página (marcadas com um asterisco vermelho) estiverem preenchidas. No ponto onde estiver, o respondente também pode clicar em "Retomar mais tarde" para salvar as respostas marcadas até então e voltar a preencher o questionário em outro momento. Após clicar em "Próximo" no último grupo de questões, haverá uma última tela com o intuito de fornecer ao respondente mais uma oportunidade de voltar e revisar todas as respostas fornecidas no questionário.

8) Recomenda-se imprimir esta página, tendo em vista que estas orientações serão úteis ao longo do preenchimento de todo o questionário.

9) Uma cópia completa deste questionário (em PDF), bem como outras informações relacionadas, estão disponíveis na página da fiscalização, hospedada no portal do TCU.

Próximo

Controle 1 - Inventário e controle de ativos corporativos

Visão geral: gerenciar ativamente (registrar, acompanhar e corrigir) todos os ativos corporativos de TI (*e.g.* equipamentos de usuários finais, incluindo computadores portáteis e dispositivos móveis; dispositivos de rede; dispositivos da Internet das Coisas [IoT]; e servidores) conectados fisicamente, virtualmente ou remotamente à infraestrutura corporativa de TI, incluindo aqueles em ambientes de nuvem (*cloud computing*), com o objetivo de conhecer com precisão todos os ativos de hardware da organização que precisam ser monitorados e protegidos. Esse gerenciamento também ajuda a identificar equipamentos não autorizados e/ou não gerenciados, os quais devem ser removidos ou corrigidos.

Este controle é importante porque, dito de maneira simples, uma organização simplesmente não é capaz de defender aquilo que sequer sabe que possui. Nesse sentido, o controle dos ativos corporativos de TI desempenha papel crítico, por exemplo, no monitoramento de segurança, na resposta a incidentes, na execução de rotinas de *backup* e no processo de recuperação de incidentes. Uma organização também deve saber quais dados são essenciais ao seu negócio e, consequentemente, identificar os ativos corporativos que mantêm ou gerenciam tais dados, de modo a aplicar-lhes controles de segurança adequados.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 1 (*Inventory and Control of Enterprise Assets*);
- ABNT NBR ISO/IEC 20000-2:2008, item 6.6.2 (Identificação e classificação dos ativos de informação);
- ABNT NBR ISO/IEC 27002:2013, item 8.1.1 (Inventário dos ativos);
- *Information Technology Infrastructure Library* (ITIL) v3, Service Transition, item 4.3 (*Service Asset and Configuration Management* – SACM);
- Instrução Normativa GSI/PR 3/2021, Capítulo II (Mapeamento de ativos de informação).

Neste ciclo do acompanhamento, serão avaliadas duas medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

1.1. Estabelece e mantém um inventário detalhado de ativos corporativos;

1.2. Trata ativos não autorizados.

Medida de segurança 1.1 - Estabelecer e manter um inventário detalhado de ativos corporativos

*1.1.1. A organização estabelece e mantém um inventário detalhado de ativos corporativos?

Por inventário detalhado de ativos corporativos, entenda-se um inventário com informações precisas, detalhadas e atualizadas sobre todos os ativos de hardware da organização que, potencialmente, armazenam, transmitem e/ou processam dados.

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*1.1.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o inventário de ativos (de hardware) existente na sua organização:

Escolha a(s) que mais se adeque(m)

- [ ] O inventário de ativos inclui dados dos equipamentos de usuários finais (incluindo computadores portáteis e dispositivos móveis)
- [ ] O inventário de ativos inclui dados dos equipamentos servidores e dos dispositivos de rede da organização
- [ ] O inventário de ativos inclui dados de dispositivos da Internet das Coisas (*Internet of Things* - IoT)
- [ ] O inventário inclui, para cada ativo, informações básicas (*e.g.* nome, endereços de rede [se estático] e de hardware [MAC *address*], proprietário/responsável, local [departamento, endereço]) e indicação se aquele ativo tem permissão/aprovação ou não para se conectar à rede da organização
- [ ] A organização utiliza uma ferramenta de *Mobile Device Management* (MDM) para auxiliá-la a gerenciar os dispositivos móveis dos usuários finais
- [ ] O inventário inclui ativos conectados à infraestrutura da organização fisicamente, virtualmente e mesmo remotamente, incluindo aqueles em ambientes de nuvem (*cloud computing*)
- [ ] O inventário inclui ativos conectados regularmente à infraestrutura de rede da organização, mesmo que não estejam sob seu controle
- [ ] As informações constantes no inventário de ativos são revisadas e atualizadas semestralmente (ou ainda mais frequentemente)

Anterior

Próximo

Controle 1 - Inventário e controle de ativos corporativos

Visão geral: gerenciar ativamente (registrar, acompanhar e corrigir) todos os ativos corporativos de TI (*e.g.* equipamentos de usuários finais, incluindo computadores portáteis e dispositivos móveis; dispositivos de rede; dispositivos da Internet das Coisas [IoT]; e servidores) conectados fisicamente, virtualmente ou remotamente à infraestrutura corporativa de TI, incluindo aqueles em ambientes de nuvem (*cloud computing*), com o objetivo de conhecer com precisão todos os ativos de hardware da organização que precisam ser monitorados e protegidos. Esse gerenciamento também ajuda a identificar equipamentos não autorizados e/ou não gerenciados, os quais devem ser removidos ou corrigidos.

Este controle é importante porque, dito de maneira simples, uma organização simplesmente não é capaz de defender aquilo que sequer sabe que possui. Nesse sentido, o controle dos ativos corporativos de TI desempenha papel crítico, por exemplo, no monitoramento de segurança, na resposta a incidentes, na execução de rotinas de *backup* e no processo de recuperação de incidentes. Uma organização também deve saber quais dados são essenciais ao seu negócio e, consequentemente, identificar os ativos corporativos que mantêm ou gerenciam tais dados, de modo a aplicar-lhes controles de segurança adequados.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 1 (*Inventory and Control of Enterprise Assets*);
- ABNT NBR ISO/IEC 20000-2:2008, item 6.6.2 (Identificação e classificação dos ativos de informação);
- ABNT NBR ISO/IEC 27002:2013, item 8.1.1 (Inventário dos ativos);
- *Information Technology Infrastructure Library* (ITIL) v3, Service Transition, item 4.3 (*Service Asset and Configuration Management* – SACM);
- Instrução Normativa GSI/PR 3/2021, Capítulo II (Mapeamento de ativos de informação).

Neste ciclo do acompanhamento, serão avaliadas duas medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

1.1. Estabelece e mantém um inventário detalhado de ativos corporativos;

1.2. Trata ativos não autorizados.

Medida de segurança 1.2 - Tratar ativos não autorizados

*1.2.1. A organização trata ativos não autorizados?

Por ativo não autorizado, entenda-se um ativo de hardware que não está registrado no inventário detalhado de ativos corporativos e que, portanto, pode representar um risco ou uma ameaça à organização.

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*1.2.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam a forma como a sua organização lida com os ativos não autorizados:

Escolha a(s) que mais se adeque(m)

- [ ] O processo de tratamento dos ativos de hardware não autorizados ocorre semanalmente (ou ainda mais frequentemente)
- [ ] Quando detectado um ativo de hardware não autorizado, este é removido da rede da organização
- [ ] Quando detectado um ativo de hardware não autorizado, além de removido, a ele são negadas futuras tentativas de conexão à rede da organização
- [ ] Quando detectado um ativo de hardware não autorizado, este é colocado em "quarentena" (ambiente especialmente configurado para evitar que possa causar qualquer dano)

Anterior

Próximo

Controle 2 - Inventário e controle de ativos de software

Visão geral: gerenciar ativamente (registrar, acompanhar e corrigir) todo software (*e.g.* sistemas operacionais e aplicativos) utilizado de modo que somente softwares autorizados possam ser instalados e executados nas máquinas, ao mesmo tempo em que quaisquer softwares não autorizados e/ou não gerenciados sejam detectados e tenham sua instalação/execução impedida.

Possuir um inventário de software completo é fundamental para a prevenção de ataques, os quais, na maioria das vezes, têm início a partir de varreduras de rede que buscam encontrar versões vulneráveis de softwares que podem ser exploradas remotamente pelo atacante. Por exemplo, se um usuário abre um *link* para um sítio malicioso utilizando uma versão vulnerável do navegador, o atacante pode instalar no computador da vítima algum programa que possibilite o seu controle remoto. Contra esse tipo de ataque, uma das principais defesas é manter todos os softwares sempre atualizados (ou seja, em versões nas quais as vulnerabilidades conhecidas já foram corrigidas) e, nesse sentido, um inventário completo ajuda a detectar se há algum software vulnerável e/ou desatualizado sendo utilizado ou, ainda, se há algum software não autorizado.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 2 (*Inventory and Control of Software Assets*);
- ABNT NBR ISO/IEC 20000-2:2008, item 6.6.2 (Identificação e classificação dos ativos de informação);
- ABNT NBR ISO/IEC 27002:2013, item 8.1.1 (Inventário dos ativos);
- ABNT NBR ISO/IEC 27002:2013, item 12.6.2 (Restrições quanto à instalação de software);
- *Information Technology Infrastructure Library* (ITIL) v3, Service Transition, item 4.3 (*Service Asset and Configuration Management* – SACM);
- Instrução Normativa GSI/PR 3/2021, Capítulo II (Mapeamento de ativos de informação).

Neste ciclo do acompanhamento, serão avaliadas três medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

2.1. Estabelece e mantém um inventário de software;

2.2. Assegura que o software autorizado seja atualmente suportado;

2.3. Trata softwares não autorizados.

Medida de segurança 2.1 - Estabelecer e manter um inventário de software

*2.1.1. A organização estabelece e mantém um inventário detalhado de software?

Por inventário detalhado de software, entenda-se um inventário com informações precisas, detalhadas e atualizadas sobre todos os softwares instalados nos ativos da organização, necessários para a realização das tarefas e rotinas corporativas diárias.

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*2.1.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o inventário de software existente na sua organização:

Escolha a(s) que mais se adeque(m)

- [ ] O inventário inclui informações básicas (*e.g.* título do software, empresa responsável [editor/*publisher*], data da instalação, respectivo propósito de negócio)
- [ ] Além das informações básicas, o inventário inclui informações adicionais sobre o software, tais como a URL (*Uniform Resource Locator*) de onde pode ser baixado, a indicação da(s) loja(s) de aplicativos, a versão, o respectivo mecanismo de implantação (*deployment*), a data de desativação etc.)
- [ ] As informações constantes no inventário de software são revisadas e atualizadas semestralmente (ou ainda mais frequentemente)

Anterior

Próximo

Controle 2 - Inventário e controle de ativos de software

Visão geral: gerenciar ativamente (registrar, acompanhar e corrigir) todo software (*e.g.* sistemas operacionais e aplicativos) utilizado de modo que somente softwares autorizados possam ser instalados e executados nas máquinas, ao mesmo tempo em que quaisquer softwares não autorizados e/ou não gerenciados sejam detectados e tenham sua instalação/execução impedida.

Possuir um inventário de software completo é fundamental para a prevenção de ataques, os quais, na maioria das vezes, têm início a partir de varreduras de rede que buscam encontrar versões vulneráveis de softwares que podem ser exploradas remotamente pelo atacante. Por exemplo, se um usuário abre um *link* para um sítio malicioso utilizando uma versão vulnerável do navegador, o atacante pode instalar no computador da vítima algum programa que possibilite o seu controle remoto. Contra esse tipo de ataque, uma das principais defesas é manter todos os softwares sempre atualizados (ou seja, em versões nas quais as vulnerabilidades conhecidas já foram corrigidas) e, nesse sentido, um inventário completo ajuda a detectar se há algum software vulnerável e/ou desatualizado sendo utilizado ou, ainda, se há algum software não autorizado.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 2 (*Inventory and Control of Software Assets*);
- ABNT NBR ISO/IEC 20000-2:2008, item 6.6.2 (Identificação e classificação dos ativos de informação);
- ABNT NBR ISO/IEC 27002:2013, item 8.1.1 (Inventário dos ativos);
- ABNT NBR ISO/IEC 27002:2013, item 12.6.2 (Restrições quanto à instalação de software);
- *Information Technology Infrastructure Library* (ITIL) v3, Service Transition, item 4.3 (*Service Asset and Configuration Management* – SACM);
- Instrução Normativa GSI/PR 3/2021, Capítulo II (Mapeamento de ativos de informação).

Neste ciclo do acompanhamento, serão avaliadas três medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

2.1. Estabelece e mantém um inventário de software;

2.2. Assegura que o software autorizado seja atualmente suportado;

2.3. Trata softwares não autorizados.

Medida de segurança 2.2 - Assegurar que o software autorizado seja atualmente suportado

*2.2.1. A organização assegura que apenas software atualmente suportado seja designado como autorizado no inventário de software?

Por software atualmente suportado, entenda-se um software previamente testado e homologado pelo setor de TI da organização.

Escolha uma das seguintes respostas:

- ○ A organização não adota essa medida de segurança
- ○ Há decisão formal ou plano aprovado para adotá-la
- ○ Adota em menor parte
- ○ Adota parcialmente
- ○ Adota em maior parte ou totalmente
- ○ Não se aplica

*2.2.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de autorização/homologação dos softwares na sua organização:

Escolha a(s) que mais se adeque(m)

- ☐ Usuários "comuns" são impossibilitados de instalar qualquer software não autorizado nas máquinas da organização
- ☐ Todo software autorizado (e, portanto, suportado) é testado e homologado previamente pelo setor de TI da organização
- ☐ Caso, para atender aos objetivos do negócio da organização, seja necessário instalar/executar algum software ainda não suportado, é documentada uma exceção justificando a necessidade, detalhando os controles mitigatórios eventualmente adotados e declarando a aceitação dos riscos residuais
- ☐ Todo e qualquer software não suportado para o qual não tenha sido documentada uma exceção é designado como "não autorizado"
- ☐ O inventário de software é revisado mensalmente (ou ainda mais frequentemente) para detectar softwares não suportados

Anterior

Próximo

Controle 2 - Inventário e controle de ativos de software

Visão geral: gerenciar ativamente (registrar, acompanhar e corrigir) todo software (*e.g.* sistemas operacionais e aplicativos) utilizado de modo que somente softwares autorizados possam ser instalados e executados nas máquinas, ao mesmo tempo em que quaisquer softwares não autorizados e/ou não gerenciados sejam detectados e tenham sua instalação/execução impedida.

Possuir um inventário de software completo é fundamental para a prevenção de ataques, os quais, na maioria das vezes, têm início a partir de varreduras de rede que buscam encontrar versões vulneráveis de softwares que podem ser exploradas remotamente pelo atacante. Por exemplo, se um usuário abre um *link* para um sítio malicioso utilizando uma versão vulnerável do navegador, o atacante pode instalar no computador da vítima algum programa que possibilite o seu controle remoto. Contra esse tipo de ataque, uma das principais defesas é manter todos os softwares sempre atualizados (ou seja, em versões nas quais as vulnerabilidades conhecidas já foram corrigidas) e, nesse sentido, um inventário completo ajuda a detectar se há algum software vulnerável e/ou desatualizado sendo utilizado ou, ainda, se há algum software não autorizado.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 2 (*Inventory and Control of Software Assets*);
- ABNT NBR ISO/IEC 20000-2:2008, item 6.6.2 (Identificação e classificação dos ativos de informação);
- ABNT NBR ISO/IEC 27002:2013, item 8.1.1 (Inventário dos ativos);
- ABNT NBR ISO/IEC 27002:2013, item 12.6.2 (Restrições quanto à instalação de software);
- *Information Technology Infrastructure Library* (ITIL) v3, Service Transition, item 4.3 (*Service Asset and Configuration Management* – SACM);
- Instrução Normativa GSI/PR 3/2021, Capítulo II (Mapeamento de ativos de informação).

Neste ciclo do acompanhamento, serão avaliadas três medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

2.1. Estabelece e mantém um inventário de software;

2.2. Assegura que o software autorizado seja atualmente suportado;

2.3. Trata softwares não autorizados.

Medida de segurança 2.3 - Tratar softwares não autorizados

*2.3.1. A organização trata softwares não autorizados?

Por software não autorizado, entenda-se um software não suportado e para o qual não tenha sido documentada, previamente, nenhuma exceção.

Escolha uma das seguintes respostas:

- ○ A organização não adota essa medida de segurança
- ○ Há decisão formal ou plano aprovado para adotá-la
- ○ Adota em menor parte
- ○ Adota parcialmente
- ○ Adota em maior parte ou totalmente
- ○ Não se aplica

*2.3.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam a forma como a sua organização lida com os softwares não autorizados:

Escolha a(s) que mais se adeque(m)

- ☐ O processo de tratamento dos softwares não autorizados ocorre mensalmente (ou ainda mais frequentemente)
- ☐ Quando detectado um software não autorizado, pode ser documentada uma exceção para autorizar seu uso, se necessário
- ☐ Quando detectado um software não autorizado e que não justifique a documentação de uma exceção, este é removido (desinstalado) do ativo

Anterior

Próximo

Controle 7 - Gestão contínua de vulnerabilidades

Visão geral: desenvolver um plano para avaliar, acompanhar e corrigir continuamente vulnerabilidades em todos os ativos na infraestrutura de TI da organização, incluindo os softwares utilizados, de modo a minimizar a janela de oportunidade para eventuais atacantes. Importante, também, monitorar constantemente fontes públicas e privadas de informações sobre novas ameaças e vulnerabilidades.

Este controle é crítico na medida em que se compreende que atacantes e defensores cibernéticos vivenciam uma disputa permanente, com os últimos sendo desafiados pelos primeiros, que procuram, constantemente, por vulnerabilidades que possam ser exploradas com sucesso. Nesse cenário, os defensores devem ter acesso tempestivo às informações disponíveis sobre as ameaças correntes e as respectivas medidas de mitigação, de modo que possam, regularmente, avaliar os ambientes das suas organizações para identificar eventuais vulnerabilidades antes dos potenciais atacantes.

No entanto, como também têm acesso às mesmas informações que os defensores, os atacantes conseguem, frequentemente, aproveitar essas vulnerabilidades mais rapidamente do que as organizações conseguem corrigi-las. Daí a importância da gestão de vulnerabilidades, atividade contínua que requer tempo, atenção e recursos. Nos dias atuais, uma organização que não avalia continuamente suas infraestruturas e softwares à procura de vulnerabilidades e proativamente corrige as falhas encontradas corre sério risco de, cedo ou tarde, ter seus ativos comprometidos.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 7 (*Continuous Vulnerability Management*);
- ABNT NBR ISO/IEC 27002:2013, item 12.6.1 (Gestão de vulnerabilidades técnicas).

Neste ciclo do acompanhamento, serão avaliadas quatro medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

7.1. Estabelece e mantém um processo de gestão de vulnerabilidades;

7.2. Estabelece e mantém um processo de correção de vulnerabilidades;

7.3. Executa a gestão automatizada de correções (*patches*) de sistemas operacionais;

7.4. Executa a gestão automatizada de correções (*patches*) de aplicativos.

Medida de segurança 7.1 - Estabelecer e manter um processo de gestão de vulnerabilidades

*__7.1.1.__ A organização estabelece e mantém um processo de gestão de vulnerabilidades?

Por processo de gestão de vulnerabilidades, entenda-se um processo de avaliação e monitoramento dos ativos corporativos e dos softwares da organização buscando, continua e proativamente, eliminar, mitigar ou corrigir as vulnerabilidades eventualmente identificadas, bem como aprimorar configurações, controles e táticas de defesa, de modo a reduzir e proteger a superfície de ataque da organização.

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*__7.1.2.__ Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de gestão de vulnerabilidades da sua organização:

Escolha a(s) que mais se adeque(m)

- [ ] O processo de gestão de vulnerabilidades está documentado
- [ ] O processo de gestão de vulnerabilidades está formalmente aprovado
- [ ] O processo de gestão de vulnerabilidades define os diversos papéis e responsabilidades associados, incluindo, por exemplo, as atividades de monitoramento de vulnerabilidades, avaliação de risco de vulnerabilidades, aplicação de correções e acompanhamento dos ativos, bem como o desempenho da função de coordenação e a documentação associada a essas atividades
- [ ] O processo de gestão de vulnerabilidades é revisado e atualizado anualmente (ou ainda mais frequentemente)
- [ ] Independentemente da revisão periódica, o processo de gestão de vulnerabilidades é atualizado sempre que a organização passa por uma mudança significativa que pode impactá-lo

Anterior

Próximo

Controle 7 - Gestão contínua de vulnerabilidades

Visão geral: desenvolver um plano para avaliar, acompanhar e corrigir continuamente vulnerabilidades em todos os ativos na infraestrutura de TI da organização, incluindo os softwares utilizados, de modo a minimizar a janela de oportunidade para eventuais atacantes. Importante, também, monitorar constantemente fontes públicas e privadas de informações sobre novas ameaças e vulnerabilidades.

Este controle é crítico na medida em que se compreende que atacantes e defensores cibernéticos vivenciam uma disputa permanente, com os últimos sendo desafiados pelos primeiros, que procuram, constantemente, por vulnerabilidades que possam ser exploradas com sucesso. Nesse cenário, os defensores devem ter acesso tempestivo às informações disponíveis sobre as ameaças correntes e as respectivas medidas de mitigação, de modo que possam, regularmente, avaliar os ambientes das suas organizações para identificar eventuais vulnerabilidades antes dos potenciais atacantes.

No entanto, como também têm acesso às mesmas informações que os defensores, os atacantes conseguem, frequentemente, aproveitar essas vulnerabilidades mais rapidamente do que as organizações conseguem corrigi-las. Daí a importância da gestão de vulnerabilidades, atividade contínua que requer tempo, atenção e recursos. Nos dias atuais, uma organização que não avalia continuamente suas infraestruturas e softwares à procura de vulnerabilidades e proativamente corrige as falhas encontradas corre sério risco de, cedo ou tarde, ter seus ativos comprometidos.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 7 (*Continuous Vulnerability Management*);
- ABNT NBR ISO/IEC 27002:2013, item 12.6.1 (Gestão de vulnerabilidades técnicas).

Neste ciclo do acompanhamento, serão avaliadas quatro medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

7.1. Estabelece e mantém um processo de gestão de vulnerabilidades;

7.2. Estabelece e mantém um processo de correção de vulnerabilidades;

7.3. Executa a gestão automatizada de correções (*patches*) de sistemas operacionais;

7.4. Executa a gestão automatizada de correções (*patches*) de aplicativos.

Medida de segurança 7.2 - Estabelecer e manter um processo de correção de vulnerabilidades

*7.2.1. A organização estabelece e mantém um processo de correção de vulnerabilidades?

Por processo de correção de vulnerabilidades, entenda-se um processo de avaliação periódica das vulnerabilidades identificadas e dos riscos a elas associados, com sua consequente priorização para correção e/ou aplicação de medidas mitigatórias, tratando primeiro as vulnerabilidades que apresentam maior risco (probabilidade x impacto) à organização, de modo a aumentar a efetividade dos esforços de proteção.

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*7.2.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de correção de vulnerabilidades da sua organização:

Escolha a(s) que mais se adeque(m)

- [ ] O processo de correção de vulnerabilidades está documentado
- [ ] O processo de correção de vulnerabilidades está formalmente aprovado
- [ ] As correções das vulnerabilidades identificadas são priorizadas de acordo com os respectivos riscos (derivados de avaliações de probabilidade e impacto no negócio, por exemplo, para cada vulnerabilidade)
- [ ] As vulnerabilidades e seus respectivos riscos são revisados mensalmente (ou ainda mais frequentemente)

Anterior

Próximo

Controle 7 - Gestão contínua de vulnerabilidades

Visão geral: desenvolver um plano para avaliar, acompanhar e corrigir continuamente vulnerabilidades em todos os ativos na infraestrutura de TI da organização, incluindo os softwares utilizados, de modo a minimizar a janela de oportunidade para eventuais atacantes. Importante, também, monitorar constantemente fontes públicas e privadas de informações sobre novas ameaças e vulnerabilidades.

Este controle é crítico na medida em que se compreende que atacantes e defensores cibernéticos vivenciam uma disputa permanente, com os últimos sendo desafiados pelos primeiros, que procuram, constantemente, por vulnerabilidades que possam ser exploradas com sucesso. Nesse cenário, os defensores devem ter acesso tempestivo às informações disponíveis sobre as ameaças correntes e as respectivas medidas de mitigação, de modo que possam, regularmente, avaliar os ambientes das suas organizações para identificar eventuais vulnerabilidades antes dos potenciais atacantes.

No entanto, como também têm acesso às mesmas informações que os defensores, os atacantes conseguem, frequentemente, aproveitar essas vulnerabilidades mais rapidamente do que as organizações conseguem corrigi-las. Daí a importância da gestão de vulnerabilidades, atividade contínua que requer tempo, atenção e recursos. Nos dias atuais, uma organização que não avalia continuamente suas infraestruturas e softwares à procura de vulnerabilidades e proativamente corrige as falhas encontradas corre sério risco de, cedo ou tarde, ter seus ativos comprometidos.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 7 (*Continuous Vulnerability Management*);
- ABNT NBR ISO/IEC 27002:2013, item 12.6.1 (Gestão de vulnerabilidades técnicas).

Neste ciclo do acompanhamento, serão avaliadas quatro medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

7.1. Estabelece e mantém um processo de gestão de vulnerabilidades;

7.2. Estabelece e mantém um processo de correção de vulnerabilidades;

7.3. Executa a gestão automatizada de correções (*patches*) de sistemas operacionais;

7.4. Executa a gestão automatizada de correções (*patches*) de aplicativos.

Medida de segurança 7.3 - Executar a gestão automatizada de correções (*patches*) de sistemas operacionais

*__7.3.1.__ A organização executa a gestão automatizada da aplicação de correções (*patches*) nos sistemas operacionais dos seus ativos?

Por aplicação de correções (*patches*), entenda-se a execução de programas de computador criados para atualizar ou corrigir um software, sanando erros de comportamento, *bugs* ou vulnerabilidades de segurança e/ou, de modo geral, melhorando sua usabilidade ou performance. *Patch*, em inglês, significa, literalmente, "remendo" <https://pt.wikipedia.org/wiki/Patch_(computa%C3%A7%C3%A3o)>.

Escolha uma das seguintes respostas:

- ○ A organização não adota essa medida de segurança
- ○ Há decisão formal ou plano aprovado para adotá-la
- ○ Adota em menor parte
- ○ Adota parcialmente
- ○ Adota em maior parte ou totalmente
- ○ Não se aplica

*__7.3.2.__ Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de aplicação de correções (*patches*) nos sistemas operacionais da sua organização:

Escolha a(s) que mais se adeque(m)

- ☐ A organização monitora constantemente fontes públicas e privadas de informações para identificar ameaças e vulnerabilidades relacionadas aos sistemas operacionais utilizados, bem como a existência de correções (*patches*) e/ou de outras formas de mitigar os riscos associados
- ☐ A organização utiliza uma ferramenta automatizada para realizar a gestão da aplicação de correções (*patches*) nos sistemas operacionais dos seus ativos
- ☐ As correções (*patches*) de sistemas operacionais são testadas e avaliadas antes de serem instaladas, de modo a assegurar que efetivamente resolvam o problema em questão e que não tragam novos riscos e/ou causem efeitos adversos intoleráveis
- ☐ A verificação da necessidade de atualização/aplicação de correções (*patches*) nos sistemas operacionais ocorre mensalmente (ou ainda mais frequentemente)

Anterior

Próximo

Controle 7 - Gestão contínua de vulnerabilidades

Visão geral: desenvolver um plano para avaliar, acompanhar e corrigir continuamente vulnerabilidades em todos os ativos na infraestrutura de TI da organização, incluindo os softwares utilizados, de modo a minimizar a janela de oportunidade para eventuais atacantes. Importante, também, monitorar constantemente fontes públicas e privadas de informações sobre novas ameaças e vulnerabilidades.

Este controle é crítico na medida em que se compreende que atacantes e defensores cibernéticos vivenciam uma disputa permanente, com os últimos sendo desafiados pelos primeiros, que procuram, constantemente, por vulnerabilidades que possam ser exploradas com sucesso. Nesse cenário, os defensores devem ter acesso tempestivo às informações disponíveis sobre as ameaças correntes e as respectivas medidas de mitigação, de modo que possam, regularmente, avaliar os ambientes das suas organizações para identificar eventuais vulnerabilidades antes dos potenciais atacantes.

No entanto, como também têm acesso às mesmas informações que os defensores, os atacantes conseguem, frequentemente, aproveitar essas vulnerabilidades mais rapidamente do que as organizações conseguem corrigi-las. Daí a importância da gestão de vulnerabilidades, atividade contínua que requer tempo, atenção e recursos. Nos dias atuais, uma organização que não avalia continuamente suas infraestruturas e softwares à procura de vulnerabilidades e proativamente corrige as falhas encontradas corre sério risco de, cedo ou tarde, ter seus ativos comprometidos.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 7 (*Continuous Vulnerability Management*);
- ABNT NBR ISO/IEC 27002:2013, item 12.6.1 (Gestão de vulnerabilidades técnicas).

Neste ciclo do acompanhamento, serão avaliadas quatro medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

7.1. Estabelece e mantém um processo de gestão de vulnerabilidades;

7.2. Estabelece e mantém um processo de correção de vulnerabilidades;

7.3. Executa a gestão automatizada de correções (*patches*) de sistemas operacionais;

7.4. Executa a gestão automatizada de correções (*patches*) de aplicativos.

Medida de segurança 7.4 - Executar a gestão automatizada de correções (*patches*) de aplicativos

*__7.4.1.__ A organização executa a gestão automatizada da aplicação de correções (*patches*) nos aplicativos (programas) dos seus ativos?

Por aplicação de correções (*patches*), entenda-se a execução de programas de computador criados para atualizar ou corrigir um software, sanando erros de comportamento, *bugs* ou vulnerabilidades de segurança e/ou, de modo geral, melhorando sua usabilidade ou performance. *Patch*, em inglês, significa, literalmente, "remendo" <https://pt.wikipedia.org/wiki/Patch_(computa%C3%A7%C3%A3o)>.

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*__7.4.2.__ Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de aplicação de correções (*patches*) nos aplicativos (programas) da sua organização:

Escolha a(s) que mais se adeque(m)

- [ ] A organização monitora constantemente fontes públicas e privadas de informações para identificar ameaças e vulnerabilidades relacionadas aos aplicativos (programas) utilizados, bem como a existência de correções (*patches*) e/ou de outras formas de mitigar os riscos associados
- [ ] A organização utiliza uma ferramenta automatizada para realizar a gestão da aplicação de correções (*patches*) nos aplicativos (programas) dos seus ativos
- [ ] As correções (*patches*) de aplicativos (programas) são testadas e avaliadas antes de serem instaladas, de modo a assegurar que efetivamente resolvam o problema em questão e que não tragam novos riscos e/ou causem efeitos adversos intoleráveis
- [ ] A verificação da necessidade de atualização/aplicação de correções (*patches*) nos aplicativos (programas) ocorre mensalmente (ou ainda mais frequentemente)

Anterior

Próximo

Controle 14 - Conscientização sobre segurança e treinamento de competências

Visão geral: estabelecer e manter um programa contínuo e permanente de conscientização e treinamento para que os colaboradores tenham conhecimentos adequados em segurança (da informação e cibernética) e, consequentemente, adotem comportamentos e procedimentos seguros de modo a reduzir os riscos para a organização.

Este controle é essencial, tendo em vista que, quando se trata do tripé da segurança da informação, formado por tecnologia, processos e pessoas, essas últimas representam, provavelmente, o principal ponto de fragilidade (no jargão da área, são "o elo mais fraco da corrente"). A título de exemplo, é bem mais fácil um invasor ter sucesso buscando induzir um usuário a clicar em um *link* ou a abrir um anexo de e-mail (e, com isso, instalar um software malicioso no computador da vítima) do que tentando explorar e aproveitar diretamente alguma vulnerabilidade de rede.

Ademais, os colaboradores, intencionalmente ou não, podem causar incidentes de segurança por meio de diversas outras ações, tais como o envio de e-mail com dados sensíveis para o destinatário errado, a perda de um equipamento/dispositivo portátil (*e.g. notebook*, *pendrive*), a utilização de senhas fracas ou a reutilização da mesma senha usada para autenticação em um sítio público.

Assim, tem-se que os programas corporativos de segurança (da informação e cibernética), em grande medida, têm seu sucesso ou fracasso determinados por essa variável (nível de conscientização e treinamento dos colaboradores), sendo que nenhum desses programas consegue reduzir os riscos da organização a níveis aceitáveis sem considerar e endereçar a componente relativa ao comportamento humano, visto que, mesmo de formas não intencionais, os usuários podem causar incidentes de segurança.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 14 (*Security Awareness and Skills Training*);
- ABNT NBR ISO/IEC 27002:2013, item 7.2.2 (Conscientização, educação e treinamento em segurança da informação);
- Norma Complementar 18/IN01/DSIC/GSIPR (Diretrizes para as atividades de ensino em Segurança da Informação e Comunicações [SIC] nos órgãos e entidades da Administração Pública Federal [APF]).

Neste ciclo do acompanhamento, serão avaliadas oito medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

14.1. Estabelece e mantém um programa de conscientização em segurança;

14.2. Treina seus colaboradores para reconhecerem ataques de engenharia social;

14.3. Treina seus colaboradores em melhores práticas de autenticação de usuários;

14.4. Treina seus colaboradores em melhores práticas de tratamento de dados;

14.5. Treina seus colaboradores para evitarem exposição não intencional de dados;

14.6. Treina seus colaboradores para reconhecerem e notificarem incidentes de segurança;

14.7. Treina seus colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos;

14.8. Treina seus colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras.

Medida de segurança 14.1 - Estabelecer e manter um programa de conscientização em segurança

*14.1.1. A organização estabelece e mantém um programa de conscientização em segurança?

Por programa de conscientização em segurança, entenda-se um programa contínuo e permanente de treinamento com vistas a mostrar aos colaboradores os riscos e ameaças aos quais os ativos e dados da organização estão sujeitos e como agir para evitá-los/mitigá-los.

Escolha uma das seguintes respostas:

- ○ A organização não adota essa medida de segurança
- ○ Há decisão formal ou plano aprovado para adotá-la
- ○ Adota em menor parte
- ○ Adota parcialmente
- ○ Adota em maior parte ou totalmente
- ○ Não se aplica

*14.1.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o programa de conscientização em segurança existente na sua organização:

Escolha a(s) que mais se adeque(m)

- ☐ O programa de conscientização em segurança está documentado
- ☐ O programa de conscientização em segurança está formalmente aprovado
- ☐ Os colaboradores recebem treinamento geral em segurança (como lidar com os ativos/dados corporativos de maneira segura) logo após sua contratação
- ☐ Os colaboradores recebem treinamento geral em segurança anualmente (ou ainda mais frequentemente)
- ☐ O programa de conscientização em segurança considera os diferentes papéis desempenhados pelos colaboradores
- ☐ Antes de assumirem novas posições na organização, os colaboradores recebem treinamento específico para os requisitos de segurança dos papéis a serem desempenhados
- ☐ O conteúdo do programa de conscientização em segurança é revisado e atualizado anualmente (ou ainda mais frequentemente)
- ☐ Independentemente da revisão periódica, o conteúdo do programa de conscientização em segurança é atualizado sempre que a organização passa por uma mudança significativa que pode impactá-lo

Anterior

Próximo

Medida de segurança 14.2 - Treinar os colaboradores para reconhecerem ataques de engenharia social

***14.2.1.** A organização treina seus colaboradores para reconhecerem ataques de engenharia social?

No contexto da segurança da informação, engenharia social refere-se à manipulação psicológica de indivíduos para que executem ações que não deveriam ou, então, que divulguem informações confidenciais, sigilosas ou sensíveis <https://pt.wikipedia.org/wiki/Engenharia_social_(seguran%C3%A7a)>.

Escolha uma das seguintes respostas:

- ○ A organização não adota essa medida de segurança
- ○ Há decisão formal ou plano aprovado para adotá-la
- ○ Adota em menor parte
- ○ Adota parcialmente
- ○ Adota em maior parte ou totalmente
- ○ Não se aplica

***14.2.2.** Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em ataques de engenharia social recebido pelos colaboradores da sua organização:

[1] *Phishing*: técnica usada para obter informações confidenciais, geralmente utilizando uma mensagem aparentemente real para enganar a vítima a digitar seus dados (*e.g.* nome de usuário, senha, detalhes do cartão de crédito) numa página falsa que imita a aparência, por exemplo, da página do banco ou da tela de acesso a algum sistema que o usuário costuma usar. Essa mensagem, alegando alguma justificativa enganosa, solicita que a vítima realize o "recadastramento" dos seus dados bancários, a alteração da sua senha eletrônica ou mesmo o cadastro para participar de um sorteio ou promoção (falsos).

[2] Pretexto (*pre-texting*): envolver a possível vítima a partir da criação de um cenário inventado (o pretexto) na tentativa de enganá-la a fornecer informações ou a realizar ações que, em circunstâncias normais, ela não forneceria/realizaria. Via de regra, o atacante fez pesquisas ou configurações prévias e, portanto, detém de antemão informações (*e.g.* data de nascimento, número do Seguro Social, valor da última conta) que lhe permitem, perante a vítima, conferir maior legitimidade ao cenário alegado. Assim, o atacante se passa por um colega de trabalho, um policial, um funcionário de banco/empresa/órgão do governo, ou seja, alguém que, pela vítima, seja percebido como uma autoridade e que, portanto, tenha direito legítimo a demandar a informação/ação em questão. Em alguns casos, o atacante só precisa de uma voz autoritária, de um tom sério e da habilidade de pensar rápido para dar respostas convincentes a eventuais perguntas da vítima.

[3] "Isca": o atacante infecta uma mídia física (*pendrive*, CD, DVD etc.) com um malware e a deixa em um local estratégico (*e.g.* estacionamento, banheiro, calçada, elevador) para ser encontrada pela vítima. Essa "isca", em geral, possui uma etiqueta atraente, com vistas a despertar a curiosidade ou a ganância da vítima (*e.g.* "Confidencial", "Salários dos Executivos Q2 2021"). Uma vez que a vítima conecte essa mídia a um computador, este *host* e as redes às quais ele estiver conectado são infectados com o malware, dando ao atacante acesso ao computador da vítima e, possivelmente, à rede interna da organização-alvo.

[4] Quiproquó (*quid pro quo*): significa, literalmente, "uma coisa por outra". Nesse tipo de ataque, o atacante promete à vítima um benefício em troca de informações ou ações. Enquanto na "isca" a vantagem vem na forma de um bem físico, no quiproquó o benefício assume a forma de um serviço. Por exemplo, um atacante ligando aleatoriamente para funcionários de uma empresa e dizendo que se trata de um retorno do setor de suporte técnico, eventualmente encontrará alguém com um problema legítimo. Assim, ao longo desse processo de "atendimento" para resolução do problema, o atacante instrui a vítima a realizar certas ações e/ou a digitar determinados comandos que instalarão um malware ou lhe darão acesso àquele computador.

[5] "Carona" (*tailgating*): uma das técnicas mais antigas de engenharia social, consiste na obtenção, por uma pessoa não autorizada, de acesso indevido a um ambiente restrito, simplesmente entrando atrás de uma pessoa que possui acesso legítimo. Por exemplo, um atacante mostrando as mãos ocupadas pode cumprimentar o funcionário legítimo e pedir-lhe que, por favor, segure a porta para ele. Se eventualmente questionado, o atacante pode mostrar bem rapidamente um cartão de acesso falso ou mesmo alegar que esqueceu ou que perdeu o próprio cartão.

Escolha a(s) que mais se adeque(m)

- ☐ O treinamento aborda ataques do tipo *phishing* [1]
- ☐ O treinamento aborda técnicas de pretexto (*pre-texting*) [2]
- ☐ O treinamento aborda técnicas de "isca" [3]
- ☐ O treinamento aborda ataques do tipo quiproquó (*quid pro quo*) [4]
- ☐ O treinamento aborda ataques do tipo "carona" (*tailgating*) [5]

Medida de segurança 14.3 - Treinar os colaboradores em melhores práticas de autenticação de usuários

***14.3.1.** A organização treina seus colaboradores em melhores práticas de autenticação de usuários?

Autenticar quer dizer confirmar que algo (ou alguém) é autêntico, real, genuíno. Assim, no contexto da segurança da informação, autenticação de usuário refere-se aos mecanismos pelos quais é possível atestar que um usuário (de determinado sistema, por exemplo) é legítimo, ou seja, que ele realmente é quem afirma ser. Em outras palavras, a autenticação está relacionada à verificação da identidade do usuário, sendo, portanto, a base da segurança em um sistema <https://pt.wikipedia.org/wiki/Autentica%C3%A7%C3%A3o>.

Escolha uma das seguintes respostas:

- ○ A organização não adota essa medida de segurança
- ○ Há decisão formal ou plano aprovado para adotá-la
- ○ Adota em menor parte
- ○ Adota parcialmente
- ○ Adota em maior parte ou totalmente
- ○ Não se aplica

***14.3.2.** Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em práticas de autenticação de usuários recebido pelos colaboradores da sua organização:

[1] Senhas consideradas seguras/fortes são aquelas que, além de possuírem um comprimento considerável, são formadas por uma combinação complexa de letras maiúsculas e minúsculas, números e caracteres especiais (símbolos). Sua importância decorre da mitigação de ataques do tipo "força bruta", nos quais o atacante tenta adivinhar a senha por meio da tentativa automatizada de todas as combinações possíveis de senhas ou, então, de um extenso arquivo pré-compilado contendo milhões de senhas (conhecido como "dicionário").

[2] Também conhecidos como gerenciadores de senhas, são aplicativos projetados para simplificar a guarda dos dados de acesso (*login*) para diversas contas *online* do usuário. No caso, o usuário só precisa configurar e lembrar de uma única senha (a chamada "senha mestra"), ficando o aplicativo responsável por definir e armazenar em um "cofre" criptografado uma senha exclusiva e forte para cada uma das contas adicionadas.

[3] Quando se trata de autenticação, há três categorias possíveis de "fatores": algo que somente você sabe (*e.g.* senha), algo que somente você possui (*e.g.* chave, crachá, *token*, celular) e algo que somente você é (*e.g.* característica biométrica). Na autenticação multifator, o usuário, para ter acesso a determinado recurso (plataforma, sistema, aplicação móvel etc.), precisa provar sua identidade utilizando fatores de verificação de ao menos duas dessas categorias (por exemplo, inserindo sua senha e, na sequência, digitando um código recebido no celular). Assim, mesmo se comprometer um desses fatores, o atacante ainda não conseguirá acessar o recurso, restando-lhe uma barreira adicional a ser superada.

Escolha a(s) que mais se adeque(m)

- ☐ O treinamento aborda dicas para composição de senhas seguras/fortes [1]
- ☐ O treinamento aborda aspectos relativos à guarda das senhas, incluindo ferramentas específicas de gerenciamento de credenciais [2]
- ☐ O treinamento aborda autenticação multifator (*multi-factor authentication* – MFA) [3]

Anterior

Próximo

Medida de segurança 14.4 - Treinar os colaboradores em melhores práticas de tratamento de dados

*__14.4.1.__ A organização treina seus colaboradores em melhores práticas de tratamento de dados?

Por meio de melhores práticas de tratamento de dados, espera-se que os colaboradores sejam capazes de identificar dados sensíveis no contexto da organização e, consequentemente, saibam como armazená-los, transferi-los, arquivá-los e destruí-los adequadamente, de modo a minimizar os riscos de vazamento.

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*__14.4.2.__ Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em práticas de tratamento de dados recebido pelos colaboradores da sua organização:

[1] "Política de mesa limpa e tela limpa": consiste em deixar as mesas de trabalho limpas de papéis, documentos, anotações e outros ativos (*e.g.* mídias removíveis, *notebooks*, *tablets*, celulares), os quais podem conter informações sensíveis, assim como as telas posicionadas fora do alcance do olhar de transeuntes e os computadores e terminais, quando não estiverem em uso, sempre desligados e/ou protegidos com mecanismo de travamento de tela/teclado ativado por tempo e controlado por senha, *token* ou outra forma de autenticação. Ao final de reuniões, apagar quadros brancos (físicos e virtuais) e descartar adequadamente os pedaços de papel utilizados (*e.g.* picotadora). Configurar impressoras com função de código PIN, de modo que apenas o próprio requerente possa pegar a sua impressão. "Uma política de mesa limpa e tela protegida reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho" (ABNT NBR ISO/IEC 27002:2013, item 11.2.9).

[2] A política de classificação da informação visa a definir diferentes níveis de proteção (com diferentes controles associados, consequentemente) para as informações da organização, levando em consideração as necessidades do negócio (quanto à confidencialidade, integridade e disponibilidade das informações), bem como requisitos legais e de conformidade. "A classificação fornece às pessoas que lidam com informações uma indicação concisa de como tratar e proteger a informação" (ABNT NBR ISO/IEC 27002:2013, item 8.2.1).

Escolha a(s) que mais se adeque(m)

- [ ] O treinamento aborda a "política de mesa limpa e tela limpa" [1]
- [ ] A organização possui uma política de classificação da informação [2] formalmente aprovada, cujo conteúdo faz parte do escopo do treinamento
- [ ] O treinamento aborda a proteção das informações contidas em ativos portáteis (*e.g. notebooks*, *tablets*, celulares, mídias removíveis), a exemplo do armazenamento apenas dos arquivos estritamente essenciais e da aplicação de mecanismos de proteção criptográfica
- [ ] O treinamento aborda aspectos relacionados à deleção permanente de arquivos e dados (*data wiping*) e ao descarte seguro de mídias/equipamentos

Anterior

Próximo

Medida de segurança 14.5 - Treinar os colaboradores para evitarem exposição não intencional de dados

*14.5.1. A organização treina seus colaboradores para evitarem exposição não intencional de dados?

Entre as causas de exposição não intencional de dados, pode-se mencionar a perda/extravio de um dispositivo portátil (*e.g. notebook*, *tablet*, celular, mídia removível), o envio de informações sensíveis ao destinatário errado ou a publicação de dados para uma audiência que não deveria ter acesso a eles.

Escolha uma das seguintes respostas:

- ○ A organização não adota essa medida de segurança
- ○ Há decisão formal ou plano aprovado para adotá-la
- ○ Adota em menor parte
- ○ Adota parcialmente
- ○ Adota em maior parte ou totalmente
- ○ Não se aplica

*14.5.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em exposição não intencional de dados recebido pelos colaboradores da sua organização:

Escolha a(s) que mais se adeque(m)

- ☐ O treinamento aborda a adoção de cuidados gerais quanto à guarda e ao uso de equipamentos portáteis (*e.g. notebooks*, *tablets*, celulares, mídias removíveis)
- ☐ O treinamento aborda a conferência dos destinatários antes do envio de comunicações (*e.g.* e-mails) que contenham informações sensíveis
- ☐ O treinamento aborda aspectos relacionados à publicação de conteúdos da organização em aplicativos de mensageria e/ou em redes sociais

Anterior

Próximo

Medida de segurança 14.6 - Treinar os colaboradores para reconhecerem e notificarem incidentes de segurança

***14.6.1.** A organização treina seus colaboradores para reconhecerem e notificarem incidentes de segurança?

Por incidente de segurança (da informação), entenda-se a ocorrência de um ou mais eventos indesejados ou inesperados com potencial para comprometer a operação do negócio e/ou colocar em risco a preservação de alguma das características da segurança das informações da organização (*e.g.* confidencialidade, integridade, disponibilidade, autenticidade) (ISO/IEC 27000:2018, item 3.31).

Escolha uma das seguintes respostas:

- ○ A organização não adota essa medida de segurança
- ○ Há decisão formal ou plano aprovado para adotá-la
- ○ Adota em menor parte
- ○ Adota parcialmente
- ○ Adota em maior parte ou totalmente
- ○ Não se aplica

***14.6.2.** Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em reconhecimento e notificação de incidentes recebido pelos colaboradores da sua organização:

[1] Precursores são sinais de que um incidente pode ocorrer no futuro. Quando detectados, a organização tem a oportunidade de prevenir a ocorrência do incidente a partir da adoção de medidas para proteger os possíveis alvos do ataque (ou, no mínimo, passará a monitorar mais atentamente a atividade desses ativos). Exemplos de precursores: i) *logs* de um servidor *web* mostrando que um escaneamento de vulnerabilidades está sendo executado; ii) anúncio de um novo *exploit* envolvendo uma vulnerabilidade no servidor de e-mail da organização; iii) ameaça de um grupo criminoso de que atacará a organização.

[2] Indicadores, a seu turno, são sinais de que um incidente pode ter ocorrido ou pode estar ocorrendo. Enquanto precursores são relativamente raros, indicadores são bastante comuns. Exemplos de indicadores: i) alerta de um sensor de detecção de intrusão de rede; ii) alerta do antivírus de que um computador foi infectado com malware; iii) nome de arquivo com caracteres estranhos percebido por um colaborador; iv) arquivo de *log* de um *host* registrando uma alteração em uma configuração de auditoria; v) múltiplas falhas de tentativas de *login* em uma aplicação a partir de um sistema remoto; vi) número significativo de e-mails devolvidos com conteúdo suspeito; vii) alteração no padrão usual de tráfego da rede (NIST *Special Publication* 800-61 *Revision* 2 – *Computer Security Incident Handling Guide*, item 3.2.2).

Escolha a(s) que mais se adeque(m)

- ☐ O treinamento aborda os principais vetores de ataque (*e.g.* mídias removíveis, sítios/e-mails maliciosos, perda/furto de equipamentos) e como cada um destes pode ser explorado
- ☐ O treinamento aborda os sinais precursores [1] e indicadores [2] da ocorrência de incidentes
- ☐ Além de ensinar os colaboradores a reconhecerem possíveis sinais da ocorrência de incidentes, o treinamento os capacita a identificarem (ou, pelo menos, terem alguma noção) o tipo, a extensão e a magnitude do problema
- ☐ Além de capacitar os colaboradores a reconhecerem incidentes de segurança, o treinamento lhes ensina os canais e os meios apropriados para a respectiva notificação

Anterior

Próximo

Medida de segurança 14.7 - Treinar os colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos

*14.7.1. A organização treina seus colaboradores para para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos?

Por falta de atualizações de segurança nos ativos corporativos, entenda-se ativos com versões de software desatualizadas e/ou sem a instalação dos pacotes de correções (*patches*) mais recentes, bem como ativos em que a execução dos processos/ferramentas automatizados de aplicação dessas correções (*patches*) tenha apresentado alguma falha/erro.

Escolha uma das seguintes respostas:

- ○ A organização não adota essa medida de segurança
- ○ Há decisão formal ou plano aprovado para adotá-la
- ○ Adota em menor parte
- ○ Adota parcialmente
- ○ Adota em maior parte ou totalmente
- ○ Não se aplica

*14.7.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em identificação e notificação da falta de atualizações de segurança nos ativos corporativos recebido pelos colaboradores da sua organização:

Escolha a(s) que mais se adeque(m)

- ☐ O treinamento capacita os colaboradores a verificarem se as versões dos softwares e dos pacotes de correções (*patches*) instalados nos ativos corporativos estão desatualizadas
- ☐ O treinamento ensina os colaboradores a reconhecerem a ocorrência de falhas na execução de processos/ferramentas automatizados (verificação de mensagens de erro, análise de *logs* etc.)
- ☐ O treinamento reforça a necessidade de notificação ao setor de TI sempre que identificada alguma das ocorrências descritas nos itens anteriores

Anterior

Próximo

Medida de segurança 14.8 - Treinar os colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras

***14.8.1.** A organização treina seus colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras?

Por rede insegura, entenda-se uma rede que não implementa medidas básicas de segurança, a exemplo da autenticação de usuários e da criptografia. Nessas redes, também costumam estar ausentes mecanismos de proteção adicionais fornecidos por soluções antivírus ou *firewalls*. Em geral, trata-se de redes abertas, que não solicitam sequer uma senha para conexão e nas quais os dados trafegados, portanto, poderão ser acessados em claro por qualquer pessoa conectada dentro do seu raio de alcance, o que representa enormes riscos para quem as acessa <https://www.finjanmobile.com/the-dangers-of-using-unsecured-wi-fi>.

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

***14.8.2.** Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras recebido pelos colaboradores da sua organização:

WEP (*Wired Equivalent Privacy*): parte do padrão IEEE 802.11 (ratificado em setembro de 1999), é popular até hoje (compatível com praticamente todos os dispositivos wi-fi disponíveis no mercado), apesar de a Wi-Fi Alliance (entidade que certifica produtos sem fio e promove a tecnologia) ter encerrado seu suporte em 2004. Como possui várias vulnerabilidades e falhas de segurança bem conhecidas e sua segurança pode ser facilmente quebrada, em questão de minutos, com um computador comum e softwares disponíveis gratuitamente, é altamente recomendado que se evite o uso deste protocolo <https://pt.wikipedia.org/wiki/Wired_Equivalent_Privacy>.

WPA (*Wi-Fi Protected Access*): desenvolvido em 2003 para melhorar a segurança do protocolo WEP (o tamanho das chaves, por exemplo, dobrou de 128 para 256 bits), reaproveitou diversos elementos do protocolo anterior para manter a compatibilidade (não tornar os dispositivos WEP obsoletos, mas atualizáveis) e, por isso, acabou mantendo alguns problemas do antecessor, a exemplo da possibilidade de ataque para descoberta da senha (porém, com menor facilidade do que no WEP) <https://pt.wikipedia.org/wiki/Wi-Fi_Protected_Access>.

WPA2 (*Wi-Fi Protected Access* II): também conhecido como padrão IEEE 802.11i, foi uma substituição da Wi-Fi Alliance, surgida em 2004, à tecnologia WPA. Esse novo padrão (802.11i) substituiu formalmente o WEP e outras características de segurança do padrão original (802.11). O WPA2 passou a utilizar o protocolo de criptografia AES (*Advanced Encryption Standard*), mais seguro do que o anterior (RC4), porém que exige, também, maior poder de processamento. Por isso, seu uso é recomendado para quem precisa de um grau maior de segurança, mas pode prejudicar o desempenho de equipamentos menos sofisticados (como os usados em redes domésticas, por exemplo) <https://pt.wikipedia.org/wiki/WPA2_(AES)>.

Escolha a(s) que mais se adeque(m)

- [ ] O treinamento aborda os riscos envolvidos na conexão de ativos corporativos a redes inseguras (*e.g.* captura de credenciais/senhas, comprometimento do ativo a partir da instalação de um malware)
- [ ] O treinamento aborda os riscos envolvidos na transmissão de dados da organização por meio de redes inseguras (*e.g.* vazamento ou adulteração dos dados, exposição indevida de dados pessoais)
- [ ] O treinamento aborda a evolução histórica dos protocolos de criptografia de redes wi-fi (WEP, WPA e WPA2), bem como suas diferenças em termos da segurança das respectivas conexões
- [ ] O treinamento capacita os colaboradores que atuam em regime de trabalho remoto a configurarem sua infraestrutura de rede local de modo a aumentarem a segurança das conexões

Controle 17 - Gestão de respostas a incidentes

Visão geral: estabelecer um programa para desenvolver e manter capacidade de resposta a incidentes de segurança da informação (*e.g.* políticas, planos, procedimentos, definição de papeis, treinamento e comunicação), de modo a estar preparado para detectar e responder rapidamente a ataques.

Tendo em vista que não se pode esperar que nenhuma organização esteja 100% protegida o tempo todo, cedo ou tarde incidentes ocorrerão. Assim, elaborar e manter um plano de resposta é essencial para que a organização esteja preparada quando isso acontecer. Os principais objetivos da gestão de respostas a incidentes, então, são identificar potenciais ameaças, responder a elas antes que se espalhem, corrigi-las antes que causem prejuízos e recuperar dados e sistemas eventualmente corrompidos.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 17 (*Incident Response Management*);
- ABNT NBR ISO/IEC 27002:2013, item 16 (Gestão de incidentes de segurança da informação), em especial subitem 16.1.5 (Resposta aos incidentes de segurança da informação);
- Norma Complementar 5/IN01/DSIC/GSIPR (Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR – nos órgãos e entidades da Administração Pública Federal [APF]);
- Norma Complementar 8/IN01/DSIC/GSIPR (Diretrizes para gerenciamento de incidentes em redes computacionais – gestão de ETIR – nos órgãos e entidades da Administração Pública Federal [APF]).

Neste ciclo do acompanhamento, serão avaliadas três medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

17.1. Designa responsáveis por gerenciar o tratamento de incidentes;

17.2. Estabelece e mantém informações de contato para reporte de incidentes de segurança;

17.3. Estabelece e mantém um processo para o recebimento de notificações de incidentes.

Medida de segurança 17.1 - Designar responsáveis por gerenciar o tratamento de incidentes

*17.1.1. A organização designa responsáveis por gerenciar o processo de tratamento de incidentes?

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*17.1.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam a designação de responsáveis por gerenciar o processo de tratamento de incidentes na sua organização:

Escolha a(s) que mais se adeque(m)

- [ ] A organização designa uma pessoa chave como responsável principal por gerenciar o processo de tratamento de incidentes (coordenar e documentar os esforços de resposta e recuperação de incidentes)
- [ ] Além de designar um responsável principal, a organização designa ao menos mais um substituto (*backup*), sendo que este último colaborador não pode se afastar simultaneamente com o primeiro
- [ ] A equipe de tratamento de incidentes é composta apenas por colaboradores da própria organização ou, caso possua funcionários terceirizados, todo o trabalho que esses realizam é supervisionado por ao menos um colaborador da organização
- [ ] As designações dos responsáveis são revisadas anualmente (ou ainda mais frequentemente)
- [ ] Independentemente da revisão periódica, as designações dos responsáveis são revisadas sempre que a organização passa por uma mudança significativa que pode impactar o processo de tratamento de incidentes

Anterior

Próximo

Controle 17 - Gestão de respostas a incidentes

Visão geral: estabelecer um programa para desenvolver e manter capacidade de resposta a incidentes de segurança da informação (*e.g.* políticas, planos, procedimentos, definição de papeis, treinamento e comunicação), de modo a estar preparado para detectar e responder rapidamente a ataques.

Tendo em vista que não se pode esperar que nenhuma organização esteja 100% protegida o tempo todo, cedo ou tarde incidentes ocorrerão. Assim, elaborar e manter um plano de resposta é essencial para que a organização esteja preparada quando isso acontecer. Os principais objetivos da gestão de respostas a incidentes, então, são identificar potenciais ameaças, responder a elas antes que se espalhem, corrigi-las antes que causem prejuízos e recuperar dados e sistemas eventualmente corrompidos.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 17 (*Incident Response Management*);
- ABNT NBR ISO/IEC 27002:2013, item 16 (Gestão de incidentes de segurança da informação), em especial subitem 16.1.5 (Resposta aos incidentes de segurança da informação);
- Norma Complementar 5/IN01/DSIC/GSIPR (Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR – nos órgãos e entidades da Administração Pública Federal [APF]);
- Norma Complementar 8/IN01/DSIC/GSIPR (Diretrizes para gerenciamento de incidentes em redes computacionais – gestão de ETIR – nos órgãos e entidades da Administração Pública Federal [APF]).

Neste ciclo do acompanhamento, serão avaliadas três medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

17.1. Designa responsáveis por gerenciar o tratamento de incidentes;

17.2. Estabelece e mantém informações de contato para reporte de incidentes de segurança;

17.3. Estabelece e mantém um processo para o recebimento de notificações de incidentes.

Medida de segurança 17.2 - Estabelecer e manter informações de contato para reporte de incidentes de segurança

*17.2.1. A organização estabelece e mantém informações de contato para reporte de incidentes de segurança?

Por informações de contato para reporte de incidentes de segurança, entenda-se relação contendo as informações de contato de todas as partes interessadas (*stakeholders*) que precisam ser informadas sobre a ocorrência de incidentes de segurança envolvendo a organização (*e.g.* colaboradores internos, funcionários terceirizados, seguradoras, agentes da lei, agências/órgãos governamentais, CTIR Gov, CERT.br).

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*17.2.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam a relação contendo as informações de contato para reporte de incidentes de segurança mantida pela sua organização:

Escolha a(s) que mais se adeque(m)

- [ ] A relação contém as informações de contato de todas as partes interessadas (*stakeholders*) que precisam ser informadas caso ocorra algum incidente de segurança (*e.g.* colaboradores internos, funcionários terceirizados, seguradoras, agentes da lei, agências/órgãos governamentais, CTIR Gov, CERT.br)
- [ ] A relação é comunicada periodicamente aos colaboradores que dela farão uso, frisando sua responsabilidade/obrigação de reportarem os incidentes de segurança às partes interessadas
- [ ] As informações de contato constantes na relação são verificadas anualmente (ou ainda mais frequentemente) para garantir que estejam sempre atualizadas

Anterior

Próximo

Controle 17 - Gestão de respostas a incidentes

Visão geral: estabelecer um programa para desenvolver e manter capacidade de resposta a incidentes de segurança da informação (*e.g.* políticas, planos, procedimentos, definição de papeis, treinamento e comunicação), de modo a estar preparado para detectar e responder rapidamente a ataques.

Tendo em vista que não se pode esperar que nenhuma organização esteja 100% protegida o tempo todo, cedo ou tarde incidentes ocorrerão. Assim, elaborar e manter um plano de resposta é essencial para que a organização esteja preparada quando isso acontecer. Os principais objetivos da gestão de respostas a incidentes, então, são identificar potenciais ameaças, responder a elas antes que se espalhem, corrigi-las antes que causem prejuízos e recuperar dados e sistemas eventualmente corrompidos.

Referências úteis:

- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 17 (*Incident Response Management*);
- ABNT NBR ISO/IEC 27002:2013, item 16 (Gestão de incidentes de segurança da informação), em especial subitem 16.1.5 (Resposta aos incidentes de segurança da informação);
- Norma Complementar 5/IN01/DSIC/GSIPR (Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR – nos órgãos e entidades da Administração Pública Federal [APF]);
- Norma Complementar 8/IN01/DSIC/GSIPR (Diretrizes para gerenciamento de incidentes em redes computacionais – gestão de ETIR – nos órgãos e entidades da Administração Pública Federal [APF]).

Neste ciclo do acompanhamento, serão avaliadas três medidas de segurança básicas relacionadas a esse controle. Especificamente, será verificado se a organização:

17.1. Designa responsáveis por gerenciar o tratamento de incidentes;

17.2. Estabelece e mantém informações de contato para reporte de incidentes de segurança;

17.3. Estabelece e mantém um processo para o recebimento de notificações de incidentes.

Medida de segurança 17.3 - Estabelecer e manter um processo para o recebimento de notificações de incidentes

*17.3.1. A organização estabelece e mantém um processo para que os colaboradores possam notificar incidentes de segurança?

Por processo para que os colaboradores possam notificar incidentes de segurança, entenda-se um processo que define requisitos mínimos, a exemplo dos atores, dos procedimentos, dos prazos e do conteúdo das notificações de incidentes.

Escolha uma das seguintes respostas:

- ( ) A organização não adota essa medida de segurança
- ( ) Há decisão formal ou plano aprovado para adotá-la
- ( ) Adota em menor parte
- ( ) Adota parcialmente
- ( ) Adota em maior parte ou totalmente
- ( ) Não se aplica

*17.3.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo para o recebimento de notificações de incidentes existente na sua organização:

Escolha a(s) que mais se adeque(m)

- [ ] O processo estabelece a responsabilidade/obrigação de os colaboradores notificarem qualquer evento de segurança da informação do qual tomem ciência e especifica o prazo para a realização da notificação, a quem a notificação deve ser encaminhada, como ela deve ser feita e quais são as informações mínimas que ela deve conter
- [ ] O processo é conhecido por e está à disposição de todos os colaboradores da organização
- [ ] O processo é revisado anualmente (ou ainda mais frequentemente)
- [ ] Independentemente da revisão periódica, o processo é revisado sempre que a organização passa por uma mudança significativa que pode impactá-lo

Anterior

Próximo

Resultados da organização:

RELATÓRIO DE *FEEDBACK*

Indicador do Controle 1 (Inventário e controle de ativos corporativos) - iControle1:

Indicador do Controle 2 (Inventário e controle de ativos de software) - iControle2:

Indicador do Controle 7 (Gestão contínua de vulnerabilidades) - iControle7:

Indicador do Controle 14 (Conscientização sobre segurança e treinamento de competências) - iControle14:

Indicador do Controle 17 (Gestão de respostas a incidentes) - iControle17:

Indicador provisório de Segurança Cibernética - iSegCiber:

Nível provisório de Segurança Cibernética - nSegCiber:

Indicadores Provisórios de Segurança Cibernética

De modo a consolidar os dados informados e oferecer ao gestor respondente um relatório de *feedback* imediato referente às atividades de segurança cibernética da sua organização, estão sendo calculados **indicadores provisórios** relativos à avaliação da organização quanto a cada um dos controles verificados neste ciclo do acompanhamento, tomados individualmente (**iControle1**, **iControle2**, **iControle7**, **iControle14** e **iControle17**), bem como quanto ao conjunto desses controles (**iSegCiber**). A sistemática de cálculo é explicada a seguir.

Para cada uma das medidas de segurança avaliadas, foram feitas duas perguntas: uma primeira do "tipo A" (questionando o grau de adoção daquela medida na organização) e uma segunda do "tipo B" (solicitando a marcação das subpráticas específicas, relativas àquela medida de segurança, que se encontram efetivamente implementadas na organização).

Nas questões do tipo A, a atribuição da nota (**provisória**) foi a seguinte, de acordo com o grau de adoção da medida de segurança na organização: 0, se a medida não é adotada ou foi considerada não aplicável; 10, se há decisão formal ou plano aprovado para adotá-la; 25, se a medida é adotada em menor parte; 50, se a medida é adotada parcialmente; e 100, se a medida é adotada em maior parte ou totalmente.

A seu turno, nas questões do tipo B as notas foram atribuídas na proporção das opções de subpráticas efetivamente marcadas (por exemplo, se há duas subpráticas e houve a marcação de apenas uma delas, a nota atribuída foi 50; se há três subpráticas e houve a marcação de duas delas, a nota atribuída foi 66).

A nota final atribuída a cada medida de segurança, então, corresponde à média ponderada das notas das duas questões correspondentes (questão do tipo A: peso 60; questão do tipo B: peso 40).

Em seguida, os valores dos indicadores atribuídos a cada um dos controles avaliados (iControle1, iControle2, iControle7, iControle14 e iControle17) foram calculados por meio da média simples das notas obtidas nas respectivas medidas de segurança.

Já o valor do indicador geral (iSegCiber) foi calculado por meio da média simples dos valores obtidos em cada um desses cinco controles (iControle1+iControle2+iControle7+iControle14+iControle17 / 5).

Assim, todos os valores de notas de questões individuais (sejam do tipo A ou do tipo B), de notas de medidas de segurança individuais, dos indicadores relativos aos controles (iControle1, iControle2, iControle7, iControle14 e iControle17) e do indicador geral (iSegCiber) variam entre 0 e 100.

Por fim, em função dos valores do iSegCiber, a organização foi **provisoriamente** enquadrada em um de quatro níveis progressivos que visam a refletir a maturidade das suas atividades de segurança cibernética (**nSegCiber**): "Inexpressivo" (iSegCiber <= 15), "Inicial" (15 < iSegCiber <= 50), "Intermediário" (50 < iSegCiber <= 80) e "Aprimorado" (iSegCiber > 80).

OBSERVAÇÃO 1: Ao gestor, relevante mesmo é ter noção das subpráticas específicas relativas a cada uma das medidas de segurança avaliadas e, se entender pertinente, programar-se para, ao longo dos próximos meses/anos, implementar na sua organização aquelas faltantes. Os indicadores e notas descritos aqui estão sendo fornecidos apenas a título de *feedback* imediato aos gestores, em caráter experimental, mas sua importância é secundária, frisando-se que a definição do nível de maturidade mais adequado a cada organização é, essencialmente, uma decisão de gestão que deve ser tomada levando-se em conta questões particulares como, por exemplo, o tipo de negócio, o apetite a riscos e o custo e a expectativa de retorno da implementação de controles internos específicos.

OBSERVAÇÃO 2: Após o término do prazo para preenchimento do questionário, a sistemática de cálculo e de atribuição dessas notas, indicadores e níveis de maturidade poderá ser alterada pelos auditores, sendo que, se isso vier a ocorrer, a nova sistemática será detalhada no relatório final deste ciclo do acompanhamento.

Por favor, registre os principais desafios, deficiências e pontos de atenção relacionados à implantação, na sua organização, dos controles e medidas de segurança questionados, bem como quaisquer outras considerações, comentários ou críticas que considerar pertinentes:

Confira suas respostas antes de clicar no botão "Enviar".

Caso ainda exista alguma pendência ou dúvida, utilize a opção "Retomar mais tarde" no canto superior direito da página para salvar as respostas fornecidas até então.

Ao final, depois do envio, aparecerá, na página de confirmação, uma opção para salvar/imprimir as respostas.

Até 22/10/2021, por meio do mesmo código de acesso (token:), é possível retornar para alterar ou complementar as respostas fornecidas.

Anterior

Enviar

OBSERVAÇÕES

1) Para cada medida de segurança, a segunda questão (do tipo B) só é mostrada caso seja marcada, na primeira questão (do tipo A), uma das seguintes opções: “Adota em menor parte”; “Adota parcialmente” ou “Adota em maior parte ou totalmente”;

2) Caso, na primeira questão, seja marcada a opção “Adota parcialmente” ou a opção “Adota em maior parte ou totalmente”, é solicitado que o gestor descreva as evidências dessa adoção;

3) Caso, na primeira questão, seja marcada a opção “Não se aplica”, é solicitado que o gestor justifique por que considera que aquela medida de segurança não se aplica à sua organização.