RANSOMWARE TASK FORCE

Plano de ação de defesa contra o ransomware

Plano de ação para as pequenas e médias empresas em matéria de mitigação, resposta e recuperação de programas de sequestro de dados.

IST Institute for SECURITY + TECHNOLOGY

Autores principais

Aaron McIntosh, Diretor de Comercialização de Produtos, ActZero
Valecia Stocchetti, Engenheira Sénior de Cibersegurança, CIS

Colaboradores

ActZero

Aaron McIntosh, Diretor de Comercialização de Produtos, ActZero

CYBER THREAT ALLIANCE

Michael Daniel, Presidente, Cyber Threat Alliance

GLOBAL CYBER ALLIANCE

Brian Cute, Diretor do Programa de Capacidade e Resiliência, Global Cyber Alliance

Leslie Daigle, Diretora de Tecnologia e do Programa de Integridade de Internet, Global Cyber Alliance

Renee McLaughlin, Responsável de Produtos, Programa de Ferramentas, Capacidade e Resiliência

VENABLE LLP

John Banghart, Diretor Sénior de Serviços de Cibersegurança, Venable LLP

CIS Center for Internet Security®

Curt Dukes, Vice-presidente Executivo, Melhores Práticas de Segurança, CIS

Phyllis Lee, Diretora Sénior de Controles, CIS

Valecia Stocchetti, Engenheira Sénior de Cibersegurança, CIS

Brian de Vallance, Assessor Sénior, CIS

IST Institute for SECURITY + TECHNOLOGY

Megan Stifel, Diretora de Estratégias, Institute for Security and Technology

resilience

Davis Hake, Cofundador de Resilience

SecurityScorecard

Sachin Bansal, Diretor de Operações e Assessor Jurídico, SecurityScorecard

Charlie Moskowitz, Vice-presidente de Assuntos Normativos e Governamentais, SecurityScorecard

Aprovado pela Iniciativa Internacional contra o Ransomware (CRI)

INTERNATIONAL COUNTER RANSOMWARE INITIATIVE CRI

Este produto não reflete as opiniões, leis ou práticas de todos os membros da Iniciativa Internacional Anti-Ransomware (CRI). Nenhum país membro está vinculado às diretrizes ou recomendações estabelecidas neste produto.

Agradecimentos

Agradecemos à Organização dos Estados Americanos e à Amazon Web Services pelo seu patrocínio e apoio à tradução.

Índice

Sumário executivo

De acordo com a Administração para a Pequena Empresa, existem 32.540.953 pequenas empresas nos Estados Unidos, representando 99,9% de todas as empresas[1]. No entanto, muitas não estão suficientemente preparadas para enfrentar o risco de um ataque cibernético. Por exemplo, um estudo de 2019 sobre o custo do crime cibernético realizado pela Accenture revelou que 43% dos ataques cibernéticos são dirigidos contra pequenas empresas, das quais apenas 14% estão preparadas para se defenderem[2]. Para abordar este risco, é cada vez mais comum que as pequenas e médias empresas (PME) obtenham seguros contra riscos cibernéticos. Contudo, cada vez mais, as seguradoras exigem que as empresas compreendam, apliquem e demonstrem melhor os métodos de gestão de riscos cibernéticos como um requisito para a aquisição de seguros contra riscos cibernéticos.

Neste contexto, recomendamos que as PME adotem um marco de cibersegurança composto pelas melhores práticas para se defenderem contra estes ataques. A implementação de um marco poderia ajudar as empresas a reforçar os seus mecanismos de defesa. Infelizmente, é difícil saber por onde começar, por isso muitas empresas ainda não sabem o que fazer e não dão prioridade às medidas de cibersegurança. Consequentemente, é necessário apresentar este marco em termos simples, com orientações práticas e de fácil compreensão. Infelizmente, algumas PME acreditam que não conseguem estabelecer marcos de cibersegurança e, portanto, perderam oportunidades de negócios para as quais precisavam de demonstrar que tinham esses marcos em vigor. Isto perpetua o ciclo de preparação ineficiente para a cibersegurança.

Em resposta à ação 3.1.1 do Relatório do Grupo de Trabalho sobre Programas de Sequestro de dados, que incentiva que as organizações de cibersegurança estabeleçam uma estrutura clara e prática para mitigação, resposta e recuperação de programas de sequestro de dados, o Grupo de Trabalho encarregado de elaborar um plano de defesa contra programas de sequestro de dados formulou um plano de ação que abrange um subconjunto de salvaguardas essenciais de higiene cibernética[3] selecionadas dos controles críticos de segurança do Centro de segurança da Internet (Controles CIS®)v8. Estas salvaguardas constituem uma norma mínima de segurança da informação que todas as empresas devem utilizar para se defenderem contra os ataques mais comuns. O Plano de ação de defesa contra os programas de sequestro de dados (ransomware) é um conjunto de salvaguardas básicas e acionáveis destinadas às PME[4].

Portanto, este plano utiliza os controles CIS, um conjunto de medidas prescritivas prioritárias desenvolvidas por uma comunidade global de especialistas em cobersegurança. O plano de ação contém 40 salvaguardas recomendadas, que foram cuidadosamente selecionadas não só porque são fáceis de aplicar, mas também devido à sua eficácia na defesa contra-ataques de sequestro de dados (ataques de ransomware). Isso foi verificado em uma análise do Modelo de Defesa Comunitária do CIS v2.0 (CIS CDM v2.0), no qual se observou que a aplicação das salvaguardas contidas neste plano constitui uma boa defesa contra mais de 70%[5]das técnicas de ataque dos programas de sequestro de dados. Deve-se notar que este plano de ação não é um guia para implementação, mas sim uma recomendação de medidas defensivas para proteger e responder a ataques de sequestro de dados e outros ataques cibernéticos comuns. No apêndice C deste documento e no folheto correspondente apresentam diversas ferramentas e recursos que podem ser utilizados para facilitar a implementação destas salvaguardas

Destinatários

O Grupo de Trabalho formulou o plano de ação especificamente para remover uma barreira crítica para as PMEs com poucos conhecimentos de cibersegurança para se defenderem contra ransomware. O plano está redigido em termos simples, com descrições de como as salvaguardas recomendadas mitigam os riscos associados

1 U.S. Small Business Advisory Office of Advocacy. Perguntas frequentes sobre PME, dezembro de 2021 https://advocacy.sba.gov/wp-content/uploads/2021/12/Small-Business-FAQ-Revised-December-2021.pdf.

2 2 Accenture. Ninth Annual Cost of Cybersecurity, março de 2019,https://www.accenture.com/us-en/insights/security/cost-cybercrime- estudar.

3 As medidas essenciais de higiene cibernética consistem nas salvaguardas do Grupo 1 de Implementação de Controles do CIS.

4 As empresas abrangem entidades dos setores público e privado.

5 Segundo o Modelo de Defesa Comunitária CIS (CDM) v2.

e fornece informações úteis para líderes empresariais e pessoal técnico que precisam trabalhar juntos para compreender os riscos e priorizar ações.

Introdução

O Grupo de Trabalho de Programas de Sequestro de dados instou a comunidade de segurança cibernética a estabelecer uma estrutura clara e prática para mitigação, resposta e recuperação. Este plano diretor baseia-se nos controles CIS, um conjunto de melhores práticas generalizadas e amplamente aceites que ajudam as empresas a concentrar os seus recursos nas medidas críticas necessárias para se defenderem contra os ataques cibernéticos mais comuns. Inclui as melhores práticas ou "salvaguardas" mais relevantes para combater programas de sequestro[6].

O CIS concebeu as salvaguardas selecionadas para as PME com pequenas equipes de TI, que têm pouca experiência em cibersegurança e muitas vezes defendem as empresas de ataques gerais e não direcionados. Estas salvaguardas constituem medidas essenciais de higiene cibernética, isto é, os controles de proteção e a capacidade básica necessária para implementar capacidades mais avançadas. O sucesso depende diretamente do planejamento e da preparação. Tal como um edifício ou um exercício de simulação de incêndio, quanto mais fortes forem os planos e as fundações, maior será a probabilidade de a empresa ser capaz de resistir a um ataque cibernético. Esses ataques podem ser rápidos e inesperados, paralisando abruptamente uma empresa despreparada.

Para ajudar as empresas a priorizar melhor as suas atividades, este plano de ação apresenta salvaguardas de dois tipos: básicas e acionáveis. As salvaguardas básicas são aquelas que uma empresa deve aplicar para tomar eficazmente quaisquer outras medidas de segurança cibernética. As salvaguardas acionáveis tomam as salvaguardas básicas como ponto de partida e reforçam o posicionamento de uma empresa em matéria cibersegurança.

Recomendamos que as PME apliquem o maior número possível destas salvaguardas. Entendemos que nem todas as empresas serão capazes de aplicar todas as salvaguardas. Embora o Grupo de Trabalho recomende a implementação total das salvaguardas do plano de ação, qualquer implementação parcial é um passo importante na melhoria da cibersegurança de uma empresa. O objetivo não é a perfeição. Se a maioria das PME adotar estes controles, as nossas empresas serão mais resilientes e ciberseguras.

Como usar este plano de ação

Os usuários devem tomar este plano de ação como ponto de partida para priorizar suas defesas de cibersegurança. O apêndice A contém uma lista completa de salvaguardas para defesa contra os ataques de sequestro de dados. Existem diversas ferramentas e recursos, encontrados no apêndice C e no folheto correspondente, para facilitar a aplicação destas salvaguardas. A inclusão de ferramentas no documento de acompanhamento não constitui nem implica de forma alguma o apoio do Grupo de Trabalho encarregado de elaborar um plano de defesa contra programas de sequestro de dados para uma solução específica, e a inclusão de ferramentas e soluções não constitui uma garantia do Grupo de Trabalho no que diz respeito à sua eficácia para fornecer cobertura de cibersegurança que melhora a proteção contra programas de sequestro de dados.

Reconhecimento de risco

Há uma forte ênfase neste plano diretor na aplicação de ações de proteção e no aumento da capacidade de implementação de capacidades mais avançadas. Embora a análise indique que as medidas essenciais de higiene cibernética constituem uma defesa contra mais de 70%[7] das técnicas de ataque utilizadas em programas de

6 Essas práticas são aquelas indicadas pelo Grupo 1 de implementação de controles do CIS v8.

7 Conforme apresentado no Modelo de Defesa Comunitária do CIS (CDM) v2.

sequestro de dados, a sua eficácia dependerá, em última análise, da forma como são aplicadas e do empenho dos adversários.

Como será visto mais adiante, as medidas essenciais de higiene cibernética representam um padrão mínimo de segurança da informação para todas as empresas e facilitam a adoção de outros controles do CIS. Esse plano diretor é o que toda empresa deveria colocar em prática para se defender dos ataques mais comuns. Para as PME, poderá ser necessário adotar mais salvaguardas para se defenderem contra os ataques mais avançados.

Plano de ação de ação

Para se defenderem contra o ransomware, as PME devem adotar uma abordagem em camadas para proteger os seus ativos mais críticos. Para esse fim, é necessário estabelecer controles em áreas como a gestão de ativos empresariais e de inventário de programas informáticos (software), gestão de vulnerabilidades, defesa contra programas maliciosos (malware), formação, recuperação de dados e resposta a incidentes. À medida que os programas de sequestro de dados evoluem, os adversários criam novas técnicas, como a extorsão. Nesses casos, os atacantes exfiltram os dados antes da encriptação e depois exigem pagamento para não os divulgarem ao público. Com as salvaguardas descritas neste plano de ação, as PME estão bem-posicionadas para se defenderem contra programas de sequestro de dados e outros tipos de ataques.

A seguir descrevemos as salvaguardas básicas e as proteções acionáveis para defesa contra programas de sequestro de dados e explicamos sua importância. **Os usuários deste plano de ação devem concentrar-se na aplicação de salvaguardas básicas antes das práticas (que são mais técnicas).**

Concordância com as funções do Marco de Cibersegurança do Instituto de Nacional de Normas e Tecnologia - NIST

Tendo em vista a ampla aceitação do conjunto de salvaguardas na administração pública, nas empresas e na comunidade de cibersegurança, o **Grupo de Trabalho encarregado de elaborar um plano de defesa contra programas de sequestro de dados** harmonizou-o com as funções do Marco de Cibersegurança do Instituto Nacional de Normas e Tecnologia (NIST) – identificar, proteger, detectar, responder e recuperar – o que facilita a execução de um programa eficaz de segurança cibernética. O agrupamento de medidas de acordo com estas funções pode ajudar as PME a compreender melhor os riscos, as medidas necessárias para se protegerem contra esses riscos, as ferramentas que podem utilizar para encontrar e detectar riscos e as soluções para conter e remediar ameaças o mais rapidamente possível.

Devido à sua complexidade e natureza técnica, as salvaguardas relacionadas com a função “detectar” não são apresentadas neste plano diretor. No entanto, o Grupo de Trabalho recomenda vivamente que as PME que seguem este plano de ação trabalhem com um prestador de serviços de cibersegurança se necessitarem de assistência no estabelecimento de detecção ou outros controles, conforme apropriado.

Visão Geral das Salvaguardas

O plano de ação abrange 40 salvaguardas: 14 básicas e 26 acionáveis. Estas medidas são primeiro agrupadas de acordo com as funções do Marco de Cibersegurança do NIST. Para cada função, o plano de ação prioriza

salvaguardas com base na sua utilidade no combate a programas de sequestro de dados e no estabelecimento de uma postura geral de defesa da cibersegurança[8].

SALVAGUARDAS BÁSICAS

As salvaguardas básicas são os componentes fundamentais do programa de cibersegurança de uma empresa. Eles também permitem a aplicação de salvaguardas acionáveis. O plano de ação apresenta 14 salvaguardas básicas prioritárias, descritas a seguir.

Identificar

Para defender a rede é preciso primeiro saber o que há nela, ou seja, qual tecnologia é utilizada e quais dados são armazenados e transmitidos. De acordo com as salvaguardas básicas que correspondem à função de identificação, recomenda-se que as PME façam e mantenham inventários de ativos e software, a fim de gerir melhor todos os dispositivos conectados e estabelecer processos de gestão de dados em que os métodos de coleta, utilização e armazenamento de dados estão claramente indicados.

Da mesma forma, deve ser feito e mantido um inventário de contas, tanto para usuários comuns quanto para aqueles com privilégios.

Estas salvaguardas são essenciais para se proteger e responder a sequestros. Sem saber quais ativos, software e contas estão na rede de uma empresa, é difícil defender-se e responder a um incidente. Por exemplo, um atacante poderia mais facilmente comprometer e usar dispositivos desconhecidos com mais facilidade no ambiente da empresa. Isso poderia agravar o risco para o negócio e prolongar o ataque ou permitir outros ataques. Conhecer o ambiente em que você opera é a base para aplicar medidas essenciais de higiene cibernética em todos os dispositivos.

Salvaguardas:

- Faça e mantenha um inventário detalhado dos ativos da empresa;
- Faça e mantenha um inventário de programas informáticos;
- Estabeleça e mantenha um processo de gestão de dados;
- Faça e mantenha um inventário de contas.

Embora estas salvaguardas sejam muito complexas, uma vez que novos ativos são constantemente adicionados à rede, elas são críticas para uma defesa eficaz e desempenham um papel crucial em outras atividades defensivas, tais como cópias de segurança e resposta a incidentes. Além disso, os dados já não estão contidos nas quatro paredes de uma empresa: dispositivos móveis e portáteis se conectam aos recursos da empresa, dificultando a gestão de dados se não forem implementadas salvaguardas adequadas.

Proteger

Depois que uma PME sabe o que há na sua rede, o próximo passo é aplicar salvaguardas aos ativos, dados e usuários para protegê-los de agentes mal-intencionados que tentam prejudicá-los.

Configurações seguras

Os processos de gerenciamento de configuração são importantes para manter a segurança ao longo do tempo. Estas salvaguardas centram-se na concepção dos dispositivos e da rede global e nas regras que regem o seu funcionamento, que em conjunto constituem a “configuração”. Eles consistem na utilização de processos de configuração seguros para ativos da empresa, como computadores portáteis, de escritório, servidores e dispositivos móveis, para citar apenas alguns. Também é importante que exista um processo de configuração da infraestrutura de rede que englobe dispositivos como corta-fogos, roteadores e comutadores. A adição de ativos empresariais, programas informáticos, usuários etc., pode aumentar o risco se não existirem processos robustos para aplicar ou reaplicar controles de segurança apropriados. Por exemplo, atualizar um programa de

8 O Grupo de Trabalho baseou a priorização na análise do marco de Táticas Adversárias, Técnicas e Conhecimento Comum de MITRE (ATT&CK).®) realizado pelo CIS e apresentado em seu Modelo de Defesa Comunitária (CDM) v2.0.

computador pode alterar um parâmetro de configuração e torná-lo menos seguro. Uma empresa deve ter um processo de configuração seguro que verifique se os ativos cumprem as configurações e normas estabelecidas e que restaure a conformidade, se necessário, para resolver desvios de segurança que possam ocorrer ao longo do tempo.

Gestão de contas e acessos

As contas de usuários podem ter tipos de acesso muito variados, desde o acesso às funções básicas, como e-mail, até contas mais privilegiadas a partir das quais você pode acessar quase tudo na empresa. As salvaguardas básicas correspondentes à função de proteção exigem que a empresa estabeleça um processo de concessão e revogação de permissões de acesso aos sistemas da empresa. Também é crucial que a empresa siga o princípio do menor privilégio, segundo o qual os usuários recebem apenas os privilégios necessários para executar uma tarefa, mesmo quando as funções de um funcionário mudam, quando são necessárias novas permissões (ou temporárias) para um projeto e quando um funcionário é admitido ou se desliga da empresa.

Planejamento de gestão de vulnerabilidades

Pesquisadores e outros interessados em segurança encontram e publicam mais de 18 mil vulnerabilidades de programas informáticos por ano. Embora haja sempre mais vulnerabilidades desconhecidas, os agentes mal-intencionados geralmente exploram primeiro as vulnerabilidades conhecidas. Portanto, a gestão de vulnerabilidades desempenha um papel crucial na proteção da infraestrutura de uma empresa. O plano de ação recomenda duas salvaguardas para estabelecer processos de gestão de vulnerabilidades e remediação de riscos, que consistem na aplicação oportuna de correções (patches) de segurança ao sistema operacional e aos aplicativos. Este processo se aplica não apenas a ativos e programas de computador, mas também aos dispositivos da rede utilizados para administrá-los ou monitorá-los.

Conscientização e formação em matéria de segurança

Embora os investimentos em tecnologia sejam importantes, as pessoas são um recurso essencial para reforçar as defesas contra programas de sequestro de dados (ransomware) e outros ataques. De acordo com o relatório[9] de investigações de violação de dados de 2021 da Verizon, 85% das violações envolveram um elemento humano. Este plano de ação recomenda que as PME estabeleçam e mantenham um programa de conscientização de segurança para todos os funcionários, parceiros e usuários terceiros. Este programa envolve não apenas treinar funcionários para interagir com as redes e sistemas da empresa de forma segura, mas também para garantir que os funcionários entendam a importância da segurança e o papel que desempenham na proteção da empresa.

Salvaguardas:

- Estabeleça e mantenha um processo de configuração seguro;
- Estabeleça e mantenha um processo de configuração seguro para infraestrutura de rede;
- Estabeleça um processo para conceder acesso;
- Estabeleça um processo para revogar o acesso;
- Estabeleça e mantenha um processo de gestão de vulnerabilidades;
- Estabeleça e mantenha um processo de correção;
- Estabeleça e mantenha um programa de conscientização de segurança.

Responder

A preparação é essencial ao responder a incidentes. Ao ter um plano antes que ocorra um incidente, a empresa sabe o que fazer caso seja atacada. As salvaguardas relacionadas à função de resposta ajudam a reduzir a interrupção das operações caso os controles falhem e o atacante consiga causar danos.

9 *2021 Verizon Data Breach Investigations Report (DBIR)* https://verizon.com/dbir.

Com base nestas salvaguardas, as empresas estabelecem processos para comunicação de incidentes e gestão de registos de segurança. No mínimo, as PME devem ter um procedimento para o pessoal notificar incidentes, descrevendo o prazo para a notificação, a quem reportar, como comunicar o incidente e as informações necessárias para a notificação. Se as empresas implementarem medidas de recuperação, poderão retomar rapidamente as operações completas para minimizar interrupções, perda de receitas e danos à marca. As empresas devem realizar periodicamente de simulações improvisadas da implementação do plano de resposta a incidentes para estabelecer as bases para o melhor resultado possível no caso de um ataque real.

Os registros também são cruciais para uma empresa responder a um incidente. O primeiro passo na gestão de registros é estabelecer um processo para que a empresa saiba quais registros devem ser coletados, no mínimo, com que frequência devem ser revisados e por quanto tempo devem ser conservados. Se sua empresa for atacada, os registros serão necessários para determinar a origem do ataque ou obter provas para fins judiciais.

Salvaguardas:

» Estabeleça e mantenha um processo de notificação de incidentes na empresa;

» Estabeleça e mantenha um processo de gestão de registros de operações.

Recuperar

Um dos maiores danos causados pelo ransomware é a perda de dados essenciais às operações de uma PME. O plano de ação inclui uma salvaguarda básica que as PME devem estabelecer e manter um processo de recuperação de dados como parte do planeamento de resposta e recuperação. Novas técnicas de ransomware (por exemplo, extorsão) representam desafios para empresas que possuem bons controles para recuperar dados, mas não os protegem, razão pela qual ambos os tipos de controles são necessários para se recuperar de um incidente de ataque de ransomware.

Salvaguardas:

- Estabeleça e mantenha um processo de recuperação de dados.

SALVAGUARDAS ACIONÁVEIS

Além das salvaguardas básicas, são necessárias outras medidas para manter eficazmente a segurança a longo prazo. Com as 26 salvaguardas acionáveis selecionadas e priorizadas no plano de ação, uma empresa pode melhorar a sua segurança e defender-se contra programas de sequestro de dados e outros ataques cibernéticos gerais e não direcionados. As salvaguardas acionáveis tomam as salvaguardas básicas como ponto de partida e consistem na aplicação dos controles técnicos necessários para proteger o meio ambiente de uma empresa.

Identificar

Como complemento às salvaguardas básicas relacionadas com a função de identificar, segundo as quais as PME devem saber quais os dispositivos e dados são utilizados no seu ambiente, a salvaguarda acionável do plano de ação para esta função exige que as PME utilizem sempre em todos os seus ativos os programas informáticos autorizados mais atualizado disponível. Os adversários examinam continuamente as redes para explorar versões vulneráveis de programas de informáticos. As vulnerabilidades nestes programas continuam a ser um dos principais vetores do ataque inicial para fins de sequestro de dados. Portanto, manter os programas

de informáticos atualizados e verificar a lista com frequência são medidas que ajudam a reduzir o risco de exploração.

Salvaguarda:

- Verifique se o software autorizado ainda é válido.

Proteger

Quase 70% das salvaguardas acionáveis no plano de ação correspondem à função de proteger. Esta função é essencial porque tem como objetivo limitar ou conter o impacto de um possível incidente de cibersegurança. As salvaguardas recomendadas estão relacionadas a aspectos técnicos e de treinamento. As salvaguardas técnicas incluem a instalação e o gerenciamento de corta-fogos (firewalls) nos servidores da empresa, a gestão da segurança de mídias removíveis e a instalação e o gerenciamento de programas antimalware, para citar apenas alguns. As salvaguardas relacionadas com a formação abordam a necessidade de ensinar o pessoal a reconhecer e reportar um ataque.

Configurações seguras

Embora os programas de sequestro de dados usem uma variedade de vetores de infecção iniciais, a maioria das tentativas de intrusão usa três: protocolo de escritório Remoto (RDP) para controle remoto de dispositivos Windows; roubo de identidade (phishing), que normalmente consiste em e-mails maliciosos que parecem vir de fontes confiáveis, mas têm como objetivo roubar credenciais ou informações confidenciais; e a exploração de vulnerabilidades de programas informáticos. Reduzir a vulnerabilidade dos ativos de rede, programas informáticos e dispositivos os defende contra esses vetores de ataque primários e fecha lacunas de segurança que poderiam persistir como resultado de configurações predefinidas inseguras. Omissões como não desativar ou encerrar contas predefinidas, não alterar as senhas predefinidas e não modificar de outros parâmetros vulneráveis aumenta o risco de exploração por um adversário. As salvaguardas nesta seção servem para que pequenas e médias empresas instalem e gerenciem um corta-fogos em servidores e gerenciem contas predefinidas nas redes e sistemas da empresa.

Também é recomendado usar as melhores práticas (por exemplo, Benchmarks CIS™ e os Guias de Implementação Técnica de Segurança da Agência de Sistemas de Informação de Defesa [DISA STIG]) para configurar sistemas com segurança.

Gestão de contas e acessos

Quando um atacante obtém credenciais para acessar uma conta, especialmente uma conta privilegiada, ele pode causar grandes danos. Ele não apenas pode invadir a rede de uma empresa, mas também pode percorrer a rede e comprometer contas e sistemas vizinhos. O plano de ação recomenda diversas atividades para reduzir o risco de comprometimento de contas, incluindo avaliações regulares de direitos de acesso privilegiado, encerramento de contas inativas, a gestão adequada de senhas para evitar a armadilha da reutilização de senhas e o uso de autenticação multifatorial em todas os sistemas da empresa. Esta última medida é especialmente importante porque cria outra camada de segurança caso uma senha seja comprometida. A gestão de contas e acessos também se aplica às plataformas de nuvem, especialmente aos serviços de correio eletrônico baseados na nuvem, que podem conectar-se a outros recursos da empresa..

Planejamento de gestão de vulnerabilidades

Os programas de sequestro de dados continuam a ser um problema para empresas que não instalam patches de segurança oportunamente para corrigir vulnerabilidades conhecidas. Vários relatórios de domínio público enfatizam que os atacantes exploram não apenas vulnerabilidades encontradas recentemente, mas também aquelas que já existem há muito tempo. O plano de ação recomenda diversas salvaguardas de gestão de vulnerabilidades, incluindo melhor gerenciamento de patches e instalação das atualizações mais recentes em sistemas e dispositivos de rede. A gestão de vulnerabilidades é especialmente importante em sistemas de geração mais antiga, que podem estar executando software obsoleto que não é mais suportado pelo fornecedor, expondo o sistema a ataques. A gestão de vulnerabilidades é especialmente importante para os sistemas de geração mais antiga, que podem estar a funcionar com software obsoleto que já não é suportado pelo

fornecedor, expondo o sistema a ataques. Se um sistema de geração mais antiga já não puder ser atualizado, devem ser adoptados outros controles para proporcionar uma proteção adequada ou substituí-lo.

As empresas devem considerar a instalação automática de patches para sistemas operacionais como Microsoft®, Windows® e Apple® macOS®. Se os patches não forem instalados automaticamente, as empresas ou seus parceiros de segurança deverão prestar atenção especial às vulnerabilidades críticas ou de dia zero anunciadas nos avisos e atualizações de segurança de cada fornecedor e implementá-las imediatamente.

Defesas contra programas maliciosos

Os programas de sequestro de dados podem ser transmitidos de diversas maneiras; por exemplo, via e-mail (através de link ou anexo), navegadores da web e mídia removível. Várias das salvaguardas do plano de ação estão relacionadas com defesas contra programas maliciosos, incluindo a instalação de ferramentas antimalware para evitar ataques contra ativos da empresa e a atualização de programas antimalware e suas definições. Também é importante manter os navegadores e clientes de correio eletrônico atualizados para evitar ataques por meio desses aplicativos. Mídias removíveis (por exemplo, cartões de memória USB) também representam um risco. Funções como início automático e reprodução automática podem permitir a execução automática de conteúdo em um sistema quando uma unidade removível for ligada ou conectada. Se uma unidade removível infectada por um programa malicioso for conectada ao sistema, ele poderá infectar o sistema alvo e os sistemas vizinhos. Desativar essas funções reduz o risco.

Outros vetores populares de programas de ransomware são URLs maliciosos, que podem ser transmitidos por e-mail ou diretamente por meio de um navegador da web. Qualquer que seja a origem do malware, controles como a filtragem de DNS podem impedir que o malware seja baixado para o sistema da vítima ou impedir que um usuário visualize uma página de roubo de identidade ou phishing (evitando assim o envio de credenciais para um atacante ou o download de um arquivo malicioso). Existem muitos serviços gratuitos de filtragem de DNS, que são uma maneira rápida e fácil de mitigar o risco de uma empresa.

Conscientização e treinamento de segurança

É extremamente importante resolver as brechas internas, como a falta de formação. Tendo em conta o crescimento implacável do roubo de identidade (phishing) e da captura ilegítima de dados sensíveis por SMS (smishing, que consiste em mensagens de texto destinadas a induzir os usuários a fornecerem informações sensíveis ou a descarregarem aplicações maliciosas), no plano de ação recomenda-se que as PME formem seus funcionários para que reconheçam e relatem ataques de engenharia social e incidentes de segurança.

Treinar a equipe para reconhecer um ataque de engenharia social é crucial para estabelecer defesas em uma rede. Embora ferramentas e tecnologia possam ser instaladas para defender a empresa contra ataques de phishing, essas ferramentas não são totalmente eficazes, portanto o pessoal da empresa é a principal linha de defesa.

É igualmente importante ensinar o pessoal a reportar incidentes de segurança. Qualquer que seja o tipo de ataque, deve ser comunicado imediatamente. A notificação imediata, seguida de ação imediata, pode interromper um ataque e deter ou reduzir os danos. O treinamento é essencial para que a equipe saiba o que fazer e como fazer.

Salvaguardas:

- Gerencie contas predefinidas em ativos e softwares da empresa;
- Use senhas exclusivas;
- Desative contas inativas;
- Restrinja privilégios de administrador a contas apenas para uso do administrador;
- Exija autenticação multifatorial para aplicativos com acesso externo;
- Exija autenticação multifatorial para acesso remoto à rede;

- Exija autenticação multifatorial para acesso administrativo;
- Automatize o gerenciamento de patches do sistema operacional;
- Automatize o gerenciamento de patches de aplicativos;
- Use apenas navegadores e clientes de e-mail totalmente vigentes;
- Use serviços de filtragem DNS;
- Mantenha a infraestrutura de rede atualizada;
- Instale e mantenha programas antimalware;
- Configure a atualização automática de definições de antimalware;
- Desative a inicialização e reprodução automática de mídias removíveis;
- Treine a equipe para reconhecer ataques de engenharia social;
- Treine a equipe para reconhecer e notificar incidentes de segurança.

Responder

Infelizmente, na prática, os melhores mecanismos de proteção são por vezes incapazes de impedir um adversário trabalhador que está disposto a gastar tempo e esforço para perturbar uma empresa. As salvaguardas acionáveis para responder consistem em notificar incidentes, estabelecer contatos importantes, saber como e quando interagir com eles, e o processo e as ferramentas necessárias para coletar e armazenar registos de forma adequada.

Ter pelo menos uma pessoa responsável pelo tratamento de incidentes facilitará a coordenação da resposta a incidentes. Essas pessoas podem ser funcionários regulares, fornecedores terceirizados ou uma combinação de ambos. Também é útil fazer uma lista de contatos para informá-los sobre o incidente, para que a empresa esteja preparada com antecedência. Os contatos podem ser funcionários regulares, autoridades policiais, seguradoras, agências governamentais, advogados ou outras partes interessadas. A comunicação é crítica durante um incidente, pois há muitas peças em movimento.

Também é importante coletar registros operacionais (logs) antes de um incidente, o que pode incluir registros de sistemas operacionais, aplicativos ou dispositivos da rede. Durante um incidente pode ser extremamente útil analisar os registros para determinar o que aconteceu. Mais importante ainda, esta análise pode ser usada para aplicar medidas de mitigação para que o ataque não volte a acontecer. O armazenamento adequado de registros também é importante, pois os arquivos de registros podem rapidamente ocupar espaço em um sistema e afetar seu desempenho.

Salvaguardas:

- Designe pessoal para lidar com a gestão de incidentes;
- Obtenha e mantenha informações de contato para relatórios de incidentes de segurança;
- Colete registros (logs) de operação;
- Armazene registros (logs) de transações de maneira apropriada.

Recuperar

Ter boas cópias de segurança (backups) de dados essenciais é uma das estratégias mais eficazes para a recuperação de um ataque de sequestro de dados. Várias salvaguardas acionáveis para recuperação de dados são prescritas no plano de ação, incluindo fazer e restaurar backups de dados. Para se recuperar de um ataque de sequestro de dados, é importante automatizar o processo de backup, proteger os dados e garantir que eles não estejam regularmente conectados à rede. Esta última medida é importante porque, mesmo que todos os

controles apropriados estejam em vigor para proteger as cópias de segurança dos dados, se as cópias forem armazenadas diretamente na rede ou no sistema sequestrado, os atacantes também encriptarão esses dados.

Salvaguardas:

» Faça backups automáticos;

» Proteja os dados de recuperação;

» Estabeleça e mantenha uma instância isolada de dados de recuperação.

Usando o plano de ação para fortalecer o seguro cibernético

A Grupo de Trabalho para Programas de Ransomware estima que em 2021 as vítimas pagaram US$ 602 milhões em extorsão com programas de sequestro de dados, o que representa um aumento de 70% em relação a 2020.

Os incidentes de sequestro de dados representaram 79% das reclamações de interrupção das operaçoes[10] e levaram a um aumento de mais de 90%, ano após ano, nos prémios de seguro[11]. Isto é insustentável tanto para os segurados como para o mercado, e é uma das razões pelas quais muitos prestadores de seguros contra riscos cibernéticos têm estado muito dispostos a apoiar o trabalho da Grupo de Trabalho sobre Programas de Ransomware.

O ciberseguro, que começou há vinte anos como uma nova cobertura para a responsabilidade civil por violações de dados, evoluiu notavelmente nos últimos dez anos e tornou-se uma ferramenta crucial para a gestão do risco cibernético empresarial. As salvaguardas básicas e acionáveis são examinadas no plano de ação. As PME podem procurar ajuda e orientação das seguradoras de riscos cibernéticos para implementar muitos destes controles. A maioria das seguradoras de risco cibernético oferece produtos proativos a preços com desconto que diminuirão significativamente o custo e a complexidade da aplicação de muitas das salvaguardas recomendadas neste plano de ação. Porém, o aumento acentuado da eficácia dos ataques de sequestro de dados de dados e a expansão da sua escala representaram um grande desafio para o mercado utilizado pelas seguradoras e outras entidades para calcular a responsabilidade decorrente de grandes incidentes de violação de dados.

O Plano de ação de Defesa contra Ransomware fornece dois elementos cruciais para a luta das companhias de seguros cibernéticos contra a intensificação desses ataques criminosos.

» Em primeiro lugar, o plano diretor fornece orientações práticas, baseadas em dados, voltadas especificamente para o mercado de pequenas e médias empresas, que muitas vezes tem mais dificuldade em defender os seus sistemas. O Grupo de Trabalho tomou as salvaguardas do Grupo 1 de Implementação de Controles Críticos de Segurança do CIS como ponto de partida e selecionou as medidas de segurança mais cruciais para a defesa contra programas de sequestro de dados. Estas medidas, que foram revistas por profissionais de seguros quanto à consistência com o que é observado nos relatórios de sinistros reais, poderiam ajudar a reduzir a probabilidade de ataques.

» Em segundo lugar, o plano de ação ajuda as companhias de seguros a compreender melhor quais os sinais que devem procurar ao segurar contas. Em outros ramos de seguros, a fixação de preços e seleção de riscos, bem como as medidas de mitigação por parte das seguradoras e resseguradoras, baseiam-se em dados de perdas baseados em engenharia. Devido ao elemento de adversários humanos e à sua natureza altamente técnica, os dados obtidos em litígios de violação de dados têm sido frequentemente utilizados no ciberseguro como base para determinar preços atuariais e diretrizes para a determinação e seleção de preços de risco. A proliferação do ransomware demonstrou claramente a necessidade de mais atenção aos controles de segurança para impedir ataques e acelerar a recuperação, para que os tomadores de seguros não sejam obrigados a pagar extorsões para recuperar rapidamente os seus sistemas críticos.

10 https://netdiligence.com/wp-content/uploads/2021/09/NetD_2021_Claims_Study_1.0_PUBLIC.pdf

11 https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html

Consistente com muitas das recomendações do plano de ação, alguns dos controles de segurança que a indústria de seguros cibernéticos observou para reduzir o custo dos incidentes e, portanto, considera no processo de garantia são os seguintes:

- bons backups;
- conscientização de segurança e treinamento em resposta a incidentes;
- mecanismos de segurança de e-mail em toda a empresa;
- proteção avançada contra malware no ponto final (endpoint);
- Visibilidade e segurança da rede.

Apresentamos vários recursos sobre resposta a incidentes no documento correspondente para que as empresas que não possuem normas de segurança bem desenvolvidos tenham um ponto de partida criado pela indústria para levar a cibersegurança a um nível superior.

Conclusão

As 40 salvaguardas recomendadas no plano de ação foram cuidadosamente selecionadas não só pela facilidade com que podem ser aplicadas, mas também pela sua eficácia na defesa contra ataques de sequestro de dados de dados. O objetivo das medidas essenciais de ciber-higiene é equipar as PME para responder a um incidente de sequestro de dados, mitigar os seus efeitos e recuperar. A aplicação do maior número possível de salvaguardas deve fazer parte de um programa iterativo de gestão de riscos em qualquer empresa. As PME que implementarem medidas essenciais de ciber-higiene estarão mais bem protegidas e bem posicionadas para se defenderem contra o ransomware. Também serão capazes de gerir o risco cibernético de forma mais eficaz e adotar os controles adicionais de que necessitam para enfrentar ameaças específicas.

Finalmente, o Grupo de Trabalho encarregado de elaborar um plano de defesa contra programas de sequestro de dados decidiu eliminar barreiras para a adopção na medida do possível. Para isso, apresentamos ferramentas e recursos que podem ser utilizados para aplicar cada uma das salvaguardas. Nos casos em que estes recursos não sejam suficientes, é aconselhável solicitar e procurar orientação junto dos prestadores de serviços de cibersegurança Embora seja impossível manter uma cibersegurança perfeita, isso pode tornar uma empresa mais resistente e resiliente às ameaças cibernéticas.

Como começar

Tal como afirmado anteriormente, o estabelecimento de um marco de segurança pode ser uma tarefa difícil para muitas PME. É importante começar aos poucos e fortalecer as defesas em um ritmo adequado para a empresa. Para começar, as empresas precisam baixar o Plano de ação de defesa contra os programas de sequestro de dados (ransomware) para determinar quais salvaguardas são recomendadas a serem adotadas. Este documento descreve as salvaguardas, bem como as funções relacionadas do Marco de Cibersegurança do NIST, e apresenta várias ferramentas e recursos que podem facilitar a implementação.

Além disso, existem muito mais ferramentas e recursos que podem facilitar a adoção de medidas essenciais de higiene cibernética nas empresas. Por exemplo, algumas empresas podem já estar a utilizando um marco de segurança e hesitam em introduzir uma diferente. Felizmente, o CIS mapeou outras estruturas de segurança (por exemplo, o marco NIST e a Certificação do Modelo de Maturidade de Cibersegurança) e fornece essas correlações gratuitamente a todas as empresas através do Navegador dos controles do

CIS e CIS WorkBench. As empresas que desejam saber mais especificamente sobre os controles CIS e especificamente como começar a aplicar este plano de ação podem consultar os seguintes recursos:

» Especificação para a avaliação dos controlos CIS: explica o que precisa ser medido para verificar se as salvaguardas do CIS foram aplicadas corretamente.

» Ferramenta de autoavaliação de controles CIS (CIS CSAT): utilizado para avaliar e monitorar a aplicação dos controles do CIS.

» Método CIS para Avaliação de Risco (CIS RAM) v2.1: um método para avaliar riscos de segurança da informação que ajuda as empresas a implementar e avaliar a sua postura de segurança em relação aos controles CIS.

No apêndice C outros recursos confiáveis são apresentados neste documento. Como já foi dito, o objetivo não é alcançar a perfeição. Qualquer avanço é essencial para avançar na adoção de medidas essenciais de higiene cibernética. Defender-se contra ransomware e ameaças cibernéticas em geral não é uma tarefa fácil, mas é uma tarefa muito necessária para fortalecer a postura de cibersegurança de empresas ao redor do mundo. O nosso Grupo de Trabalho está confiante de que as salvaguardas selecionadas facilitarão a defesa contra programas de sequestro de dados e outros ciberataques e ajudarão a estabelecer uma base sólida para uma defesa ciberdefesa eficaz.

Apêndice A. Plano de Ação para Programas de Defesa Contra Sequestro de dados (ransomware)

Categoria	Número de salvaguarda CIS	Função de Segurança do NIST	Título de salvaguarda CIS	Tipo
Identificar				
Conheça seu ambiente	1.1	Identificar	Faça e mantenha um inventário detalhado dos ativos da empresa	Básico
	2.1	Identificar	Faça e mantenha um inventário de programas de computador	Básico
	2.2	Identificar	Verifique se o software autorizado ainda é válido	Acionável
	3.1	Identificar	Estabeleça e mantenha um processo de gerenciamento de dados	Básico
	5.1	Identificar	Faça e mantenha um inventário de contas	Básico
Proteger				
Configurações seguras	4.1	Proteger	Estabeleça e mantenha um processo de configuração seguro	Básico
	4.2	Proteger	Estabeleça e mantenha um processo de configuração seguro para a infraestrutura da rede	Básico
	4.4	Proteger	Instale e gerencie um firewall nos servidores	Acionável
	4.7	Proteger	Gerencie contas predefinidas em ativos e software da empresa	Acionável
Gestão de contas e acessos	5.2	Proteger	Use senhas exclusivas	Acionável
	5.3	Proteger	Desative contas inativas	Acionável
	5.4	Proteger	Restrinja os privilégios de administrador para as contas para uso exclusivo do administrador	Acionável
	6.1	Proteger	Estabeleça um processo para conceder acesso	Básico
	6.2	Proteger	Estabeleça um processo para revogar o acesso	Básico
	6.3	Proteger	Exija autenticação multifatorial para aplicativos com acesso externo	Acionável
	6.4	Proteger	Exija autenticação multifatorial para acesso remoto à rede	Acionável
	6.5	Proteger	Exija autenticação multifatorial para acesso administrativo	Acionável
Planejamento da gestão de vulnerabilidade	7.1	Proteger	Estabeleça e mantenha um processo de gestão de vulnerabilidades	Básico
	7.2	Proteger	Estabeleça e mantenha um processo de correção (patches)	Básico
	7.3	Proteger	Automatize o gerenciamento de patches do sistema operacional	Acionável
	7.4	Proteger	Automatize o gerenciamento de patches de aplicativos	Acionável
	12.1	Proteger	Mantenha a infraestrutura da rede atualizada	Acionável
Defesa contra programas maliciosos	9.1	Proteger	Use apenas navegadores e clientes de e-mail que sejam totalmente válido	Acionável
	9.2	Proteger	Use serviços de filtragem DNS	Acionável
	10.1	Proteger	Instale e mantenha programas antimalware	Acionável
	10.2	Proteger	Configure a atualização automática de definições de antimalware	Acionável
	10.3	Proteger	Desative a inicialização automática e a reprodução automática de mídias removíveis	Acionável
Conhecimento segurança e treinamento	14.1	Proteger	Estabeleça e mantenha um programa de conscientização de segurança	Básico
	14.2	Proteger	Treine a equipe para reconhecer ataques de engenharia social	Acionável
	14.6	Proteger	Treine a equipe para reconhecer e relatar incidentes de segurança	Acionável
Detectar				
Responder				
Recuperação de dados e resposta a incidentes	17.1	Responder	Designe pessoal para lidar com o gerenciamento de incidentes	Acionável
	17.2	Responder	Obtenha e mantenha informações de contato para relatórios de incidentes de segurança	Acionável
	17.3	Responder	Estabeleça e mantenha um processo de notificação de incidentes na empresa	Básico
	8.1	Responder	Estabeleça e mantenha um processo de gestão de registros (logs) operações	Básico
	8.2	Responder	Colete logs de operação	Acionável
	8.3	Responder	Armazene logs de transações de maneira apropriada	Acionável

Categoria	Número de salvaguarda CIS	Função de Segurança do NIST	Título de salvaguarda CIS	Tipo
Recuperar				
Recuperação de dados e resposta incidentes	11.1	**Recuperar**	Estabeleça e mantenha um processo de recuperação de dados	Básico
	11.2	**Recuperar**	Faça backups automáticos	Acionável
	11.3	**Recuperar**	Proteja os dados de recuperação	Acionável
	11.4	**Recuperar**	Estabeleça e mantenha uma instância isolada de dados de recuperação	Acionável

Apêndice B. Abreviações e siglas

CIS	Center for Internet Security (Centro de Segurança na Internet)
CIS CDM	Center for Internet Security Community Defense Model
Controles CIS	Controles críticos de segurança do Center for Internet Security
CIS CSAT	Center for Internet Security ControlsSelf Assessment Tool
CIS RAM	Center for Internet Security Risk Assessment Method
CISA	Cibersecurity and Infrastructure Security Agency (Agência de Cibersegurança e Segurança da infraestrutura)
CMMC	Cibersecurity Maturity Model Certification (Certificação do Modelo de Maturidade de Cíbersegurança)
CSF	Cybersecurity Framework
DISA STIGs	Defense Information Systems Agency Security Technical Implementation Guides
DNS	Domain Name System (Sistema de Nomes de Domínio)
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
GCA	Global Cyber Alliance
IG	Implementation Group
IG1	Implementation Group 1
IR	Incident Response
IT	Information Technology
ISO	International Organization for Standardization
IST	Institute for Security and Technology
MFA	Multi-factor authentication
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge (Táticas Adversárias, Técnicas e Conhecimento Comum da MITRE)
MS-ISAC	Multi-State Information Sharing and Analysis Center (Centro Multiestadual de Intercâmbio e Análise de Informação)
NIST	National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia)
RDP	Remote Desktop Protocol
RTF	Ransomware Task Force
PME	Pequenas e médias empresas
SLTT	State, Local, Tribal, and Territorial governments
URL	uniform resource locator (localizador uniforme de recursos, ou seja, o endereço de um site)
USB	universal serial bus (barramento serial universal)

Apêndice C. Recursos Suplementares

Centro de Controles Críticos de Segurança da Internet (Controles CIS) v8: contém mais informações sobre verificações do CIS; explica como começar e por que cada controle é crítico; apresenta os procedimentos e ferramentas a serem utilizados para implementação e uma lista completa de salvaguardas para cada controle.

Especificação para a avaliação dos controles CIS: explica o que precisa ser medido para verificar se as salvaguardas do CIS foram aplicadas corretamente.

Navegador de controles CIS: mostra a correlação de controles e salvaguardas com outras normas de segurança (por exemplo, CMMC, NIST SP 800-53 Rev. 5, MITRE ATT&CK).

Ferramenta de autoavaliação de controles CIS (CIS CSAT): É utilizado para avaliar e monitorar a aplicação dos controles do CIS.

Modelo Defesa da Comunidade CIS (CDM) v2.0: guia publicado pelo CIS que aproveita a ampla disponibilidade de resumos completos de ataques e incidentes de segurança e usa a estrutura MITRE ATT&CK, um ecossistema endossado pela indústria.

Método CIS para Avaliação de Risco (CIS RAM) v2.1: um método para avaliar riscos de segurança da informação que ajuda as empresas a implementar e avaliar a sua postura de segurança em relação aos controles CIS.

Filiação no SecureSuite de CIS: acesso ao CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks e outras. Filiação gratuita para governos estaduais, locais, tribais e territoriais.

Benchmarks CIS™: diretrizes para a configuração segura de mais de 100 tecnologias, incluindo sistemas operacionais, aplicativos e dispositivos da rede.

Orientação conjunta da Agência de Cibersegurança e de Infraestrutura (CISA) e do Centro Multiestado de Intercâmbio e Análise de Informação (MS-ISAC®) sobre programas de sequestro de dados: melhores práticas e recomendações sobre programas de sequestro de dados com base no conhecimento da CISA e MS-ISAC®.

CISA | Stop ransomware: o balcão único do governo dos Estados Unidos para acabar com os programas de sequestro de dados.

Cyber Readiness Institute | Ransomware Playbook: como se preparar para lidar com um ataque de sequestro de dados, responder e se recuperar.

Guias de implementação técnica de segurança da Agência de Sistemas de Informação de Defesa (DISA) STIG): normas de configuração desenvolvidos pela Agência de Sistemas de Informação de Defesa.

Filiação ao Centro de Intercâmbio e Análise de Informações sobre Infraestrutura Eleitoral (EI-ISAC®): gratuito para todas as entidades estaduais, locais, tribais e territoriais que trabalham com autoridades eleitorais dos EUA e suas associações.

Departamento Federal de Investigação (FBI) | Ficha informativa sobre programas de sequestro de dados: o que são os ransomware e o que fazer a respeito.

Global Cyber Alliance (GCA) | Ferramentas de cibersegurança para pequenas empresas: ferramentas gratuitas e eficazes que podem ser usadas hoje para tomar medidas imediatas para reduzir o risco cibernético.

Instituto de Segurança e Tecnologia (IST) | Relatório do Grupo de Trabalho sobre Programas de Sequestro de dados: marco de ação abrangente: principais recomendações do Grupo de Trabalho sobre Programas de Sequestro de dados.

Filiação ao MS-ISAC: gratuito para todos os 50 estados, o Distrito de Columbia, os territórios dos EUA, governos locais e tribais, escolas públicas de ensino fundamental e médio, instituições públicas de ensino superior, autoridades e outras entidades públicas não federais nos Estados Unidos.

Marco de Cibersegurança do Instituto Nacional de Normas e Tecnologia (NIST): https://www.nist.gov/cyberframework.

Espaço do NIST para a Cibersegurança das Pequenas Empresas, página de programas de sequestro de dados: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/programas de sequestro de dados.

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org