Cartilha de Cibersegurança

Um guia rápido para Micro e Pequenas Empresas (MPEs)

International Digital Dialogues
Shaping digital policy together

Esta cartilha foi elaborada no âmbito do Diálogo Digital Brasil-Alemanha e conta com apoio das seguintes entidades:

Publicado por:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Projeto Global Diálogos Digitais
Edifício Brasília Trade Center, sala 1501
Asa Norte, 70711-902
Brasília - DF, Brasil
E-mail: digital-dialogues@giz.de

Projeto gráfico e diagramação:
Gustavo Bonifácio
Créditos da foto:
Adobe Stock
Em nome de:
Ministério Federal Alemão para Digital e Transporte (BMDV)
Brasília, Brasil 2023

O Ministério Federal Alemão para Digital e Transporte (BMDV) contratou a Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH para implementar o Projeto Global Diálogos Digitais.
Esta publicação baseia-se no guia "Cyber-Sicherheit für KMU Die TOP 14 Fragen[1]", produzido pelo Departamento Federal para Segurança da Informação (BSI) da Alemanha.

Federal Ministry for Digital and Transport

Implemented by giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

1 Cyber-Sicherheit für KMU - Die TOP 14 Fragen (bund.de)

Sumário

INTRODUÇÃO 4

PARTE I: AVALIAÇÃO DE VULNERABILIDADE 6

PARTE II: MEDIDAS DE MITIGAÇÃO DE RISCOS 8

Pergunta 1: Quem é o responsável? 9

Pergunta 2: Você usa antivírus? 10

Pergunta 3: Quão bem você conhece o seu sistema de TI? 10

Pergunta 4: Você realiza regularmente *backups* de dados? 12

Pergunta 5: Você faz atualizações regularmente? 13

Pergunta 6: Você desativou os macros? 13

Pergunta 7: Você tem alguma política estabelecida para senhas seguras? 14

Pergunta 8: Como você protege suas contas de e-mail? 16

Pergunta 9: Como você separa as diferentes áreas de TI? 16

Pergunta 10: Você tem controle sobre os riscos de TI no *home office* e em viagens de negócios? 17

Pergunta 11: Como você se informa e informa seus funcionários? 19

Pergunta 12: Sua apólice de seguro também cobre riscos cibernéticos? 19

Pergunta 13: Você configurou um firewall? 20

Pergunta 14: Você sabe como reagir a um ataque cibernético? 20

Pergunta 15: Você treina para a emergência? 22

PARTE III: GERENCIAMENTO DE INCIDENTES E RECUPERAÇÃO 23

1. Introdução

Sejamos francos: a maioria das micro e pequenas empresas (MPEs) no Brasil e no mundo não possuem um nível adequado de cibersegurança. Muitas empresas estão cientes que necessitam reforçar suas barreiras de segurança da informação. No entanto, mesmo quando o desejo de melhoria está presente, a implementação de medidas práticas para melhorar a segurança é frequentemente considerada uma empreitada trabalhosa e complexa tecnicamente.

Segundo dados do Núcleo de Informação e Coordenação do Ponto BR (NIC.br),

> // APENAS 37% DAS PEQUENAS EMPRESAS BRASILEIRAS POSSUEM POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO. //

Em contrataste, esta porcentagem sobe para 63% e 74% em empresas de médio e grande porte, respectivamente. Enquanto as grandes corporações frequentemente possuem departamentos dedicados à segurança da TI, MPEs estão involuntariamente mais expostas a ataques cibernéticos devido à falta de recursos. Sendo assim, essas empresas carecem de mais apoio e orientação sobre como protegerem-se.

Diante desse cenário, esta publicação busca abordar o tema de forma prática e simplificada, distanciando-se de aspectos teóricos complexos e aproximando-se da realidade de micro e pequenas empresas. Vamos esquecer por um momento as normas ISO e da ABNT e começar com os conceitos básicos mais importantes de segurança de TI, de forma breve e concisa, com base em 15 perguntas. Uma vez dado o primeiro passo, os próximos já não serão tão difíceis.

Ao final da leitura, você saberá o que pode ser implementado internamente em sua empresa e o que deve ser terceirizado. Aliás, esse é um ponto importante: você não precisa fazer tudo sozinho na área de TI/segurança. O importante é que as medidas necessárias sejam implementadas. Caso não seja possível fazer tudo internamente, é recomendável encontrar um profissional de TI na sua região que possa te ajudar nesta empreitada.

E se, ao ler isso, você pensar "Ah, não entendo todos estes termos técnicos!", não se preocupe. Você não precisa saber como uma tecnologia funciona para entender a importância dela, basta ter ouvido o termo uma vez. Por exemplo, se você não conhece a palavra airbag, não notará se o seu carro dos sonhos não tiver um

MPEs como um importante fator econômico

No Brasil, o conceito de micro, pequenas e médias empresas é assegurado pela Lei Geral das Microempresas e Empresas de Pequeno Porte, que visa proteger e aumentar a competividade de pequenos negócios, fortalecendo a economia como um todo. Segundo a Lei Geral, a microempresa pode ter um faturamento anual de até R$360 mil ao ano e, no caso da pequena empresa, de até R$ 4,8 milhões.

> // PEQUENOS NEGÓCIOS E EMPREENDEDORISMO ESTÃO MUITO PRESENTES NA SOCIEDADE E NA ECONOMIA BRASILEIRAS, CORRESPONDENDO A APROXIMADAMENTE 99% DAS EMPRESAS DO PAÍS //

30% do Produto Interno Bruto (PIB) brasileiro e cerca de 78% das novas vagas de emprego. O Atlas dos Pequenos Negócios no Brasil, publicado anualmente pelo Sistema Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE), divulgou que pequenos negócios são responsáveis pela circulação de R$ 35 bilhões por mês na economia brasileira.

Por que a segurança cibernética importa?

Segundo o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o Brasil é o segundo país que mais sofre ciberataques nas Américas. Infelizmente, a adoção de tecnologias digitais no país, tanto nos pequenos negócios como no setor público, não foi acompanhada pela conscientização da importância da segurança cibernética para a economia e para sociedade como um todo.

Atualmente, a Secretaria de Segurança da Informação e Cibernética (SSIC) do GSI é o órgão do governo federal que acumula mais responsabilidades e competências em relação à cibersegurança no país. A SSIC é responsável pela coordenação da atividade nacional de segurança da informação, incluindo a formação e qualificação de recursos humanos na área.

Entretanto, o Brasil ainda carece de uma coordenação de ações e esforços que enderecem os problemas advindos da área de segurança cibernética. Esse cenário prejudica o surgimento de esforços conjuntos entre os diferentes setores interessados em promover uma cultura de segurança cibernética no país. Visando suprir esta lacuna no âmbito do Executivo, o governo federal publicou o Decreto nº 11.856, de 26 de dezembro de 2023, que institui a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança (CNCiber). O Decreto visa incrementar, por meio da PNCiber, a atuação coordenada e o intercâmbio de informações de segurança cibernética entre os diferentes âmbitos do governo, o setor privado e a sociedade em geral.

Já na Alemanha, o Escritório Federal de Segurança da Informação (BSI) é o ponto central para tratar de temas relacionados à cibersegurança. O BSI defende que, para resolver o problema da conscientização nas empresas, é necessário pensar primeiramente na forma como as pessoas se relacionam no ciberespaço.

Uma pesquisa do BSI indicou que a principal ameaça aos sistemas de controle industrial são erros humanos e sabotagem, seguidos de infiltração de *malware*[1], engenharia social e *phishing*[2]. Diante do resultado da pesquisa, especialistas na área, como por exemplo o Centro de Competência em Segurança Industrial da Associação Alemã de Fabricação de Máquinas e Instalações Industriais (**VDMA**) passaram a instruir suas empresas associadas a investirem em treinamento e conscientização de funcionários como política prioritária para melhorar os níveis internos de cibersegurança. Mais informações sobre os tipos de ataques utilizando engenharia social podem ser encontrados no portal para a cibersegurança da VDMA[3].

// A PESQUISA DO BSI, BEM COMO A MUDANÇA NO DIRECIONAMENTO DA VDMA, DEMONSTRA COMO MEDIDAS SIMPLES PODEM SER MUITO EFICAZES PARA TORNAR EMPRESAS MAIS SEGURAS NO AMBIENTE DIGITAL. //

Esse cenário é especialmente válido para pequenos negócios, que podem implementar treinamentos e políticas rotineiras em suas empresas sem demandar investimentos elevados em soluções técnicas.

[1] Termo genérico para qualquer tipo de *software* malicioso projetado para prejudicar ou explorar qualquer dispositivo. O *malware* é utilizado pelos criminosos para obter alguma forma de ganhos financeiros de suas vítimas.

[2] Golpe que induz a vítima a clicar em um *link* malicioso por meio de ferramentas de mensagem, como e-mail e WhatsApp. O objetivo do golpe é obter informações confidenciais como número de cartão de crédito e senhas de login.

[3] Risk for companies: How hackers use social engineering as an effective attack method - Enterprise Cybersecurity (unternehmen-cybersicherheit.de)

Parte I

Parte I: Avaliação de Vulnerabilidade

Esta seção propõe uma autoavaliação rápida para que MPEs possam verificar seu grau de exposição aos ataques cibernéticos.

A verificação pode ser realizada a partir de um questionário curto baseado no guia *Cyber-Sicherheit für KMU*[4], produzido pelo Departamento Federal para Segurança da Informação (BSI) da Alemanha. O guia é composto por 14 perguntas para avaliação de vulnerabilidade.

No decorrer da elaboração desta cartilha, especialistas da área sugeriram a inclusão de uma pergunta extra que visa o treinamento regular de processos operacionais relacionados à segurança da TI, totalizando 15 perguntas. As perguntas estão organizadas em ordem progressiva de complexidade de implementação, ou seja, as primeiras perguntas podem ser solucionadas facilmente e já garantem um nível básico de cibersegurança para sua empresa.

// FAÇA A CHECAGEM! A SUA EMPRESA JÁ É CAMPEÃO DE SEGURANÇA CIBERNÉTICA OU AINDA TEM POTENCIAL PARA MELHORIA? //

Na parte II desta cartilha, há uma breve explicação sobre cada pergunta com possíveis medidas e recursos externos que podem ser úteis para você se educar mais no tema.

Perguntas para autoavaliação:

- Pergunta 1: Quem é responsável pela segurança cibernética na empresa?
- Pergunta 2: Você usa programas antivírus?
- Pergunta 3: Quão bem você conhece seus sistemas de TI?
- Pergunta 4: Você faz *backup* dos seus dados periodicamente?
- Pergunta 5: Você faz atualizações regularmente?
- Pergunta 6: Você desabilitou os macros?
- Pergunta 7: Você tem alguma política estabelecida para senhas seguras?
- Pergunta 8: Como você protege suas contas de e-mail?
- Pergunta 9: Como você separa as diferentes áreas de TI?
- Pergunta 10: Você tem os riscos de TI sob controle no escritório, em casa e durante viagens de negócios?
- Pergunta 11: Como você se informa e informa seus funcionários sobre riscos cibernéticos?
- Pergunta 12: Sua apólice de seguro também cobre riscos cibernéticos?
- Pergunta 13: Você configurou um *firewall*?
- Pergunta 14: Você sabe como reagir em caso de um ciberataque?
- Pergunta 15: Você treina regularmente ações relacionadas à segurança cibernética?

[4] Cyber-Sicherheit für KMU - Die TOP 14 Fragen (bund.de)


Administation
HUB
Profits
Current projections & Expected targets
Market density and control
Stacks movement
Cashflow rotation
Company's Assets and their growth
Copyright - All rights reserved

Parte II

Parte II: Medidas de Mitigação de Riscos

Nesta seção, você encontrará um conjunto de medidas que podem ser colocadas em prática para aumentar o nível de cibersegurança de sua PME e, consequentemente, diminuir sua exposição aos ataques cibernéticos.

As medidas estão organizadas em grau progressivo de dificuldade de implementação, ou seja, as medidas relativamente à pergunta 1 podem ser executadas facilmente e requerem pouco ou nenhum investimento financeiro. Conforme as perguntas avançam, as medidas adquirem maior grau de complexidade, como treinamentos e simulações de ciberataques. Recomendamos que você leia esta parte com atenção e adapte as medidas para o contexto da sua PME.

Pergunta 1: Quem é o responsável?

Quem na minha empresa é responsável pela cibersegurança?" Esta pergunta deve ser respondida em primeiro lugar se você deseja lidar com a segurança do seu sistema de TI. A resposta é a mesma em todos os casos: a gestão, ou, em outras palavras, a liderança da empresa!

Se os sistemas de TI de uma empresa falham (por exemplo, devido a um ataque de *ransomware*[5] bem-sucedido), ela entra em colapso na maioria das vezes. Nada mais é produzido, as mercadorias não são mais entregues, os pedidos não são mais aceitos, os prazos dos clientes não são mais cumpridos. Isso resulta em perda de receitas e custos contínuos.

Se os dados dos clientes (o que é quase sempre o caso em ataques de *ransomware*) forem roubados e divulgados, a reputação da empresa pode ser destruída.

Em outras palavras, a situação é grave. Esse não é um tópico que a gestão deve delegar para baixo.

Conscientização da gestão

É claro que a gestão da empresa não precisa conhecer os detalhes dos sistemas de TI, mas o tema da segurança da informação deve ser uma pauta regular nas reuniões da diretoria. Talvez não com a mesma frequência que os itens "Finanças" ou "Vendas", mas pelo menos regularmente.

Se você é membro da gestão da empresa: ótimo, então você já está ciente! Se não for, certifique-se de que sua gestão saiba o mais rápido possível! Se não conseguir provocar essa mudança interna, busque ajuda de associações ou organizações comerciais para que possam organizar eventos para promover outras ações sobre "cibersegurança" que tenham gestores como público-alvo.

Informe-se sobre os riscos que se aplicam às empresas brasileiras, leia mais sobre gerenciamento de riscos e padrões avançados de segurança e entenda melhor o ambiente legislativo em relação à proteção de dados neste guia elaborado pela BRASSCOM[6].

Responsabilidade pela implementação de medidas definidas

É preciso deixar claro qual departamento na empresa é responsável pela operação do sistema de informações e qual departamento é responsável pela segurança da informação.

Em pequenas empresas, a mesma pessoa frequentemente será responsável por esses dois processos. Já em empresas maiores, idealmente as responsabilidades devem ser separadas nas duas áreas.

[5] Um tipo de *malware* que bloqueia o dispositivo e exige um resgate para desbloqueá-lo.

[6] BRASSCOM 2022: Segurança da Informação e Segurança Cibernética - Brasscom

A experiência mostra que a segurança às vezes só pode ser alcançada ao sacrificar o conforto do usuário. Por esse motivo, é comum que gerentes de TI e o responsável pela segurança cibernética discordem entre si. Portanto, não é uma boa ideia que eles estejam em diferentes níveis hierárquicos. Se os dois não conseguem entrar em acordo, aplica-se novamente a mesma regra: a gestão é a responsável! É a gestão que decidir qual o nível de segurança ideal para a empresa e quais riscos residuais podem ser aceitos.

Pergunta 2: Você usa antivírus?

Sim, antivírus são programas (*softwares*[7]) muito úteis para proteger recursos de TI: eles podem bloquear *malware* e evitar ataques de ransomware, portanto, devem ser instalados em todos os sistemas, principalmente aqueles conectados à Internet (computadores de trabalho, servidores de arquivos, etc.).

O antivírus protege contra ameaças conhecidas que evoluem rapidamente: centenas de milhares de novas variantes de *malware* são lançadas todos os dias. Sendo assim, o antivírus em si e seu banco de dados de detecção devem ser mantidos sempre atualizados. Esse banco de dados permite a identificação de programas e arquivos maliciosos. Se o *software* não for atualizado regularmente, sua eficácia da proteção será rapidamente comprometida.

Os programas antivírus disponíveis no mercado (alguns já inclusos no sistema operacional) oferecem atualizações automáticas e verificação automática de arquivos. Essas configurações devem necessariamente ser ativadas em todos os dispositivos da empresa.

Além disso, especialmente para pequenas empresas, pode valer a pena assinar as funcionalidades extras oferecidas pelos fabricantes de *software* antivírus, como *firewall*, filtro da *web*, VPN, ferramentas *anti-phishing* e ferramentas para reforçar a segurança de transações bancárias. A adesão a essas funcionalidades depende da finalidade da empresa e também dos recursos disponíveis.

É importante lembrar: instalar um bom antivírus e acreditar que, com isso, todas as preocupações de segurança de TI estão resolvidas é coisa do passado. O antivírus é importante, mas os outros pontos dessa lista são ainda mais importantes.

Pergunta 3: Quão bem você conhece o seu sistema de TI?

Eu conheço os sistemas de TI, aplicativos e dados vitais do meu negócio?". Para se proteger adequadamente, cada empresa, até mesmo um microempreendedor individual, deve conhecer seu *hardware*[8] e *software*, bem como os dados e processos que são a base de seus ativos de informação e que contribuem para a continuidade da empresa.

Esse inventário pode ser usado para desenvolver medidas de proteção apropriadas. Isso pode parecer mais trabalho do que realmente é, mas, na verdade, pode ser feito rapidamente em uma pequena empresa.

[7] Sistema de processamento de dados, programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador.

[8] Conjunto dos componentes físicos de um computador.

Lista de todos os componentes utilizados

Devem ser listados e colocados em um inventário: computadores, *smartphones*, *tablets*, servidores locais, servidores remotos (para hospedagem de sites, serviços de comunicação, aplicativos especializados etc.). Além disso, todos os dispositivos periféricos também devem ser inventariados: impressoras, scanners, roteadores, switches, modems de banda larga móvel, etc. Dessa forma, você sabe o que precisa ser protegido e, posteriormente, pode identificar os elementos críticos para a atividade da empresa.

Lista de *softwares* em uso

Você deve conhecer o tipo de *software*, suas funções essenciais e a versão específica que está sendo usada. É importante ter licenças de usuário válidas e ter os códigos de registro prontamente disponíveis e, de preferência, impressos em uma pasta de arquivos ou em um hard drive físico desconectado da rede da empresa, pois isso é essencial para a manutenção e reinstalação do *software*.

Lista de dados e processamento de dados

Pense no que aconteceria se dados fossem perdidos, alterados ou tornados inutilizáveis. Quais dados colocariam em risco o funcionamento do seu negócio ou até mesmo interromperiam suas atividades? Você possui um arquivo de clientes? Onde os dados são armazenados, por exemplo, dados contábeis? Quais dados estão sujeitos a regulamentações legais?

A mesma pergunta se aplica ao processamento dos dados: se comprometidos, quais procedimentos de processamento de dados prejudicariam gravemente ou até mesmo interromperiam a atividade da empresa?

Pense em dados e processamento de forma mais ampla e tente inserir isso dentro do contexto da sua empresa. Uma base de dados não é necessariamente um grande repositório em um *software* complexo, pode ser um *excel* em que você os dados cadastrais de seus clientes e fornecedores, por exemplo. E processamento de dados é qualquer atividade que diga respeito aos dados, como coletar e armazenar as informações dos clientes.

Listagem de todas as permissões de acesso

Nessa etapa, será definido quem pode utilizar o sistema de informações e quais são as condições para cada tipo de acesso: categoria do usuário (administradores, usuários, convidados) e tipo de acesso (conexão local ou remota). Essa listagem garante que nenhum acesso não autorizado seja realizado (por exemplo, por ex-funcionários que possam ter saído da empresa em conflito ou ex-prestadores de serviços), reduzindo assim a probabilidade de ataques acontecerem.

Listagem das conexões de TI com o mundo exterior

Quais são os pontos de contato entre o sistema de informações da sua empresa e a Internet? Cada acesso à Internet por meio de um provedor ou parceiro deve ser identificado e registrado no inventário. Isso permite a aplicação de filtros adequados e regras de monitoramento.

Essa listagem é necessária porque permite que a empresa identifique suas necessidades e capacidades no ambiente digital. Ela deve ser atualizada regularmente (pelo menos duas vezes por ano).

Além disso, a listagem pode ajudar a encontrar soluções de TI adequadas para a empresa, identificar medidas de segurança necessárias e, se necessário, criar uma visão detalhada com um provedor de serviços contratado para aumentar ainda mais a segurança. Também é muito útil para os profissionais responsáveis por tomarem medidas de contra-ataque em caso de ciberataque.

Pergunta 4: Você realiza regularmente *backups* de dados?

Backups são cópias de segurança dos dados e realizá-los regularmente permite retomar as atividades empresariais mais rapidamente após um incidente, especialmente após um ataque de ransomware.

Identifique os dados que devem ser copiados

Para identificar os dados relevantes, é necessário primeiro inventariar todos os sistemas de processamento de dados e determinar quais dados são essenciais para suas operações comerciais. Isso pode incluir dados organizacionais (por exemplo, arquivos de clientes ou o conhecimento prático dos processos de fabricação) e dados técnicos, como a configuração de computadores individuais ou toda a infraestrutura empresarial, incluindo equipamentos de produção industrial.

Determine a frequência dos *backups*

O intervalo entre os *backups* deve ser definido com base na quantidade de dados digitais gerados em um determinado período. Por exemplo, pequenas empresas no setor de artesanato podem precisar fazer *backups* semanais de faturas e arquivos de clientes, enquanto empresas de médio porte que vendem produtos ou serviços online podem necessitar de *backups* diários.

Também é possível ter uma abordagem diferenciada para *backups*, com pontos de salvamento diferentes: diariamente para dados comerciais e semanalmente para dados técnicos, como sistemas operacionais e arquivos de configuração.

Escolha um meio de armazenamento adequado para os dados

Isso pode incluir um meio físico, como um disco rígido externo que deve ser desconectado do sistema de informações após o *backup*, ou um serviço de *backup* em nuvem. Para seus dados mais valiosos, você pode optar por utilizar ambos. Um dispositivo físico que é conectado ao sistema apenas durante o *backup* oferece a vantagem de não permitir acessos externos (especialmente de *ransomware*). No entanto, ele pode ser roubado, danificado (por exemplo, em um incêndio ou inundação) ou apresentar falhas técnicas. Os serviços em nuvem permitem automatizar facilmente os *backups*, mas podem apresentar riscos de acesso não autorizado ou instabilidades.

Independentemente do método escolhido, todos os *backups* devem ser testados quanto à integridade e funcionalidade imediatamente após sua criação. Isso garante que, em caso de necessidade, todos os dados relevantes possam ser restaurados com sucesso. Se você possui um seguro contra ataques cibernéticos, isso provavelmente será exigido pela seguradora. Isso ocorre porque é comum que empresas restaurem dados de *backups* após um incidente de TI e descubram que os dados são inutilizáveis.

Verifique quais dados devem ser criptografados

A criptografia dos dados antes do armazenamento é uma prática recomendada. É especialmente importante para dados armazenados na nuvem ou em dispositivos móveis, pois ela protege os dados em caso de acesso não autorizado.

É importante verificar a escolha do provedor de nuvem, os métodos de armazenamento de dados e os requisitos de acesso e autenticação. Mesmo para *backups* locais (disco rígido externo, *pen drive*, fita magnética), é recomendável criptografar os dados. Importante: se você estiver realizando *backups* criptografados (o que é sempre uma boa ideia), certifique-se de armazenar uma cópia segura da chave de criptografia em algum lugar.

Os sistemas operacionais comumente utilizados no ambiente corporativo geralmente incluem recursos de criptografia de dados, mas geralmente precisam ser ativados explicitamente.

Pergunta 5: Você faz atualizações regularmente?

A maioria dos invasores explora vulnerabilidades públicas e documentadas para invadir sistemas de informação. Eles causam danos aproveitando-se da negligência dos usuários e/ou explorando vulnerabilidades em serviços conectados à Internet, como servidores de e-mail, *firewalls*[9], etc. É importante atualizar os sistemas operacionais e o *software* de aplicativos assim que as atualizações de segurança forem disponibilizadas pelos respectivos fabricantes.

As atualização de segurança não têm custo e podem ser programadas para dias e horários específicos a fim de não atrapalhar as atividades cotidianas da empresa. Não atualizar, por outro lado, frequentemente custa muito para a empresa. A falta de atualizações ou atualizações atrasadas é uma das principais razões para ataques cibernéticos bem-sucedidos contra MPEs.

Use soluções de *hardware* e *software* atualizadas

Por hábito, negligência ou para economizar dinheiro, pode ser tentador manter *hardware* ou *software* além de seu "ciclo de vida", ou seja, por mais tempo do que o período em que o fabricante ou provedor garante a manutenção em condições seguras. *Hardwares* ou *softwares* que não podem mais ser atualizados devem ser descartados ou desinstalados. É recomendável amortizar o investimento nestes programas ainda durante a vida útil para poder adquirir novos produtos quando for necessário.

Ativar atualizações automáticas

As atualizações do sistema operacional e de todos os *softwares* utilizados devem ser aplicadas assim que uma atualização for disponibilizada pelos fabricantes. Isso é especialmente válido para todos os sistemas conectados à Internet. Para garantir que os sistemas estejam sempre atualizados, é recomendado ativar as funções de atualização automática fornecidas pelos provedores.

Além das atualizações regulares, atualizações fora do cronograma regular podem ser necessárias quando alguma vulnerabilidade crítica é descoberta e requer atualização imediata, ao invés de esperar várias semanas até o próximo ciclo de atualização. Essas atualizações também devem ser aplicadas o mais rápido possível.

Defina quem é responsável pelo processo de atualização

Se você contratou um provedor de serviços de TI, certifique-se de que ele atualize os sistemas de TI utilizados em sua empresa. Se necessário, exija que isso seja explicitamente incluído no contrato de serviços. Se você não terceirizou essa tarefa para um provedor de serviços externo, certifique-se de que alguém em sua empresa seja claramente designado para essa tarefa.

Pergunta 6: Você desativou os macros?

Por que você deve desativar os macros?

Uma das principais formas de entrada para *ransomware* são os macros embutidos em anexos de e-mails. Você pode fechar essa porta de entrada gratuitamente!

[9]Dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permiter ou bloquear tráfegos específicos de acordo com um conjunto definido de regras e segurança.

Macros são pequenos programas que podem ser incorporados em arquivos, como documentos do Word, *Excel*, PowerPoint ou PDF. Eles permitem automatizar processos, o que pode ser útil em algumas aplicações. Infelizmente, isso também se aplica a invasores que desejam assumir o controle do seu sistema de TI.

Ao abrir um arquivo que contém um macro, o programa geralmente solicita permissão ao usuário. O problema é que a maioria dos usuários não consegue avaliar se o arquivo que estão abrindo é legítimo ou não.

Criminosos cibernéticos frequentemente enviam seu *software* malicioso usando endereços de e-mail de remetentes conhecidos e confiáveis para os destinatários. Muitas vezes, o assunto do e-mail malicioso se refere a uma conversa de e-mail existente (o que geralmente significa que o suposto remetente também foi vítima do *software* malicioso).

Não deixe a decisão de permitir ou não a execução de macros nas mãos dos usuários - eles simplesmente não têm o conhecimento necessário para tomar essa decisão. Proíba (por exemplo, nas Políticas de Grupo do Windows) a execução de macros de forma geral. A maioria das pequenas e médias empresas não usa macros de qualquer maneira.

E, se o fizerem, seu administrador pode assinar os macros necessários e permitir sua execução. No entanto, todos os outros macros devem continuar proibidos. Isso pode ser feito com apenas alguns cliques do mouse.

Pergunta 7: Você tem alguma política estabelecida para senhas seguras?

Por que se deve escolher senhas seguras?

Muitos ataques na Internet são facilitados pelo uso de senhas simples ou repetidas em diferentes serviços. Existem diferentes tipos de ataques a senhas: ataques de força bruta (o atacante tenta o maior número possível de combinações) ou ataques de dicionário (o atacante tenta as senhas mais comuns, como nomes populares ou combinações simples como "qwertz").

Os ataques também podem envolver engenharia social: o atacante tenta usar informações pessoais, como os nomes de seus parentes ou os apelidos de seus animais de estimação, que ele encontrou anteriormente em redes sociais.

É ainda mais fácil tentar senhas que já estão disponíveis online. Talvez sua senha (juntamente com muitas outras) tenha vazado em algum serviço A, porque ele não tinha uma boa segurança em seu banco de dados. Se você usar a mesma senha no serviço B, isso facilitará a vida do atacante.

Além disso, um ataque pode não se limitar ao serviço afetado, mas pode se espalhar dentro da empresa ou para seus parceiros. Por exemplo, seu endereço de e-mail pode ser usado pelo atacante para enviar e-mails maliciosos aos seus contatos comerciais, levando-os a realizar ações prejudiciais (como clicar em um *link* para um site infectado que parece ser completamente legítimo, como o do seu banco).

Essa técnica de ataque é chamada de *phishing*, um dos métodos mais comuns para obter senhas de outras pessoas.

O que é uma senha segura?

Ao escolher uma senha, sua criatividade não tem limites. O importante é que você consiga se lembrar bem dela. Existem diferentes estratégias para ajudar nisso: uma pessoa pode lembrar-se de uma frase e usar apenas a primeira letra de cada palavra (ou a segunda ou a última).

Em seguida, pode-se transformar certas letras em números ou caracteres especiais (? ! % + @ $ #), etc).

Outra opção é usar uma frase inteira como senha ou combinar diferentes palavras usando caracteres especiais. Outra possibilidade é escolher aleatoriamente cinco ou seis palavras do dicionário e combiná-las. Isso resulta em uma senha fácil de lembrar, fácil de digitar e difícil de ser quebrada por atacantes.

Em geral, quanto mais longa, melhor. Uma boa senha deve ter pelo menos oito caracteres. Idealmente, ela também deve conter caracteres especiais e números. Para métodos de criptografia de redes sem fio, como WPA2 ou WPA3, por exemplo, a senha deve ter pelo menos 20 caracteres. Nessas situações, ataques offline são possíveis, mesmo sem uma conexão de rede em andamento.

Geralmente, todas as combinações de caracteres disponíveis podem ser usadas para criar uma senha, como letras maiúsculas e minúsculas, números e caracteres especiais. Alguns provedores de serviços online têm requisitos técnicos sobre os caracteres permitidos ou a serem usados. Se o seu sistema permitir caracteres especiais, leve em consideração que, ao viajar para o exterior, pode ser que esses caracteres não possam ser digitados em teclados típicos do país.

Não são adequadas como senhas os nomes de membros da família, de animais de estimação, de melhores amigos, de celebridades, datas de nascimento etc. A senha completa não deve ser encontrada em dicionários. Além disso, ela não deve ser baseada em variações comuns ou padrões de repetição ou teclado, como "asdfgh" ou "1234abcd". Não é recomendável simplesmente adicionar números ao final da senha ou incluir um dos caracteres especiais usuais no início ou final de uma senha simples. Os programas comuns de quebra de senhas automatizadas conseguem identificar esses padrões.

Como deve ser uma boa política de senhas

- Uma senha diferente deve ser usada para cada serviço que requer autenticação. Acima de tudo, nunca use a mesma senha para o e-mail pessoal e o e-mail profissional.

- Um gerenciador de senhas pode ajudar a gerar senhas fortes e a lembrá-las. Com um gerenciador de senhas, todas as senhas podem ser armazenadas em um arquivo criptografado, que pode ser acessado com uma única senha exclusiva. E você só precisa se lembrar dessa única senha.

- Para que uma boa política de senhas seja eficaz, os usuários devem estar cientes dos riscos de escolher uma senha fácil de ser adivinhada. Se o provedor de serviço (e-mail, banco, etc.) oferecer autenticação multifator (MFA/2FA), ela deve ser ativada. Muitos serviços já permitem fortalecer a senha com autenticação de dois fatores: além da senha, é necessário fornecer um segundo fator. Sem esse segundo fator, um atacante geralmente não conseguirá aproveitar sua senha de forma alguma. Por exemplo, os bancos utilizam o SMS ou o método de *push-TAN* para a autenticação de dois fatores, em que um código de segurança é exibido no celular. É recomendado ativar sempre esse tipo de autenticação quando ela for oferecida.

Autenticação de múltiplos fatores (MFA)

Idealmente, a autenticação de múltiplos fatores deve ser implementada com um *token* físico (cartão de chip, *token* USB/FIDO2, cartão de identificação etc.) para simplificar o acesso.

Pequenas e médias empresas que possuem muitas soluções de *software* centralizadas (sistema de comunicação, serviços da *web* internos, etc.) podem simplificar e fortalecer os mecanismos de autenticação ativando o *Single Sign-on* (SSO), que permite que uma vez logado, o acesso seja válido para todos os serviços utilizados pela empresa.

Para controlar e verificar a aplicação dessas regras, as MPEs podem adotar as seguintes medidas, entre outras:

- Bloquear contas após várias tentativas de login malsucedidas, podendo ser temporária ou permanentemente;
- Desativar opções de login anônimo ("contas de visitantes");
- Implementar uma política sólida de senhas nos servidores de autenticação, impedindo senhas fracas.

Pergunta 8: Como você protege suas contas de e-mail?

Micro empresas

E-mails são o vetor de infecção mais comum em computadores no local de trabalho, seja através da abertura de anexos contendo código malicioso ou clicando em um *link* que redireciona para um site malicioso (*phishing*).

Algumas perguntas simples podem pelo menos parcialmente proteger contra ataques por *e-mail*: Você conhece o remetente? Você espera alguma informação dele?

O *link* proposto está relacionado ao assunto mencionado? Em caso de dúvida, é necessário verificar com o remetente a autenticidade da mensagem por meio de outro canal, como telefone, WhatsApp, SMS etc.

Além disso, é essencial evitar o redirecionamento de mensagens profissionais para uma conta de e-mail pessoal, pois muitas vezes a rede da empresa está melhor protegida do que a dos funcionários em casa.

Empresas de pequeno e médio porte

Independentemente de a empresa operar seu próprio sistema de e-mail ou contratar o serviço, é necessário garantir:

- Que os correios dos usuários tenham um scanner antivírus pré-instalado para filtrar arquivos infectados;
- Que a comunicação entre os computadores dos usuários e os servidores que hospedam as caixas de correio eletrônico (da empresa ou servidores públicos) esteja criptografada.

Medidas organizacionais, como conscientização dos funcionários, devem ser rigorosamente implementadas para se proteger contra ações fraudulentas, por exemplo, solicitação de transferência de dinheiro supostamente proveniente de um superior.

Pergunta 9: Como você separa as diferentes áreas de TI?

A conexão de aplicativos de TI com a Internet traz uma série de riscos, incluindo:

- Transferência não autorizada (exfiltração) de dados da empresa para terceiros, comprometendo a confidencialidade das informações e prejudicando a reputação da empresa, caso venha a se tornar público.
- Invasões que comprometem a integridade e/ou disponibilidade do sistema de informação e dos recursos de produção da empresa, especialmente por meio de ***ransomware***.
- Roubo de identidade.

- Uso indevido do sistema de informações da empresa para fins fraudulentos ou criminosos.

Como você pode se proteger melhor contra essas ameaças?

Não utilize contas de grupo, mas sim contas de usuário individuais para cada funcionário. Usuários normais não devem ter privilégios de administrador. Contas de administrador devem ser reservadas para administradores, como gerentes e colaboradores responsáveis pela segurança cibernética. Isso reduz o risco de infiltração de códigos maliciosos.

Para navegar na Internet, apenas contas de usuário devem ser usadas. De fato, muitos ataques são causados pelo fato de navegar a partir de uma conta com privilégios de administrador, o que facilita muito para um invasor obter controle total sobre o computador.

As contas de administrador devem ser usadas exclusivamente para configurar sistemas ou instalar *softwares*. As contas e suas permissões devem ser atualizadas regularmente.

Quando os funcionários deixam a empresa, seus direitos de acesso devem ser identificados e revogados, de modo que nem eles nem terceiros possam usar esses direitos novamente.

O ideal é usar um computador apenas para trabalho e não para assuntos pessoais ou familiares. Se isso não for possível e o mesmo dispositivo for usado por várias pessoas, é necessário criar contas de usuário adicionais para cada uso adicional.

Um empresário individual pode facilmente implementar essas divisões em seu próprio dispositivo.

O mesmo se aplica a dispositivos móveis: as permissões de aplicativos devem ser restritas para cada tipo de uso, e os aplicativos devem ser baixados apenas de plataformas oficiais ou do site dos verdadeiros desenvolvedores.

Pequenas e médias empresas

Pequenas e médias empresas com um número maior de funcionários e com uma rede de TI com vários dispositivos devem tomar as seguintes medidas ou implementá-las por meio de um provedor de serviços terceirizado:

- As conexões entre os computadores devem ser proibidas por padrão. Se um computador estiver infectado com *malware*, essa segmentação impede que os outros computadores sejam imediatamente infectados também.

- Para administração da rede da empresa, devem ser usados apenas computadores e contas de administrador designados especificamente para esse fim.

- Se os recursos da empresa permitirem, as atividades de TI da empresa devem ser divididas em diferentes zonas de rede por meio de filtros físicos ou virtuais (áreas separadas para servidores internos, servidores conectados à Internet, computadores de trabalho, de administração, sistemas industriais etc.). É recomendável buscar orientação de especialistas em TI para desenvolver uma arquitetura segura e adaptada ao seu sistema de informações e ao tipo de dados que você possui.

Pergunta 10: Você tem controle sobre os riscos de TI no *home office* e em viagens de negócios?

Laptops, *smartphones* ou *tablets* são práticos para uso em *home office* e em viagens de negócios. Muitas tarefas podem ser realizadas enquanto estiver em movimento ou em casa. Embora o trabalho remoto facilite a continuidade dos negócios, também apresenta certos riscos.

O que deve ser considerado ao viajar a negócios?

- Faça *backup* de seus dados para que possa recuperá-los em caso de perda ou roubo dos dispositivos.
- Equipe seus dispositivos com filtros de privacidade durante viagens de negócios.
- Certifique-se de que suas senhas não sejam armazenadas em locais de segurança duvidosa, por exemplo, no navegador da *web*, e não sejam oferecidas automaticamente, mas precisem ser inseridas pelo usuário.
- Use autenticação de múltiplos fatores (como um cartão inteligente ou um *token* FIDO2).
- Se possível, criptografe seus dados sensíveis ou todo o disco rígido.
- Permita o acesso à rede da empresa de fora (por exemplo, do *home office*) apenas por meio de VPN (Rede Privada Virtual). Isso também se aplica ao acesso às contas de *e-mail* por meio do navegador da *web*.

Quais precauções devem ser tomadas durante o uso?

- Mantenha seus dispositivos, mídias de armazenamento e arquivos sempre com você, mesmo se você apenas sair rapidamente para ir ao banheiro ou pegar um café, por exemplo.
- Informe imediatamente sua empresa caso perca seus dispositivos ou este sejam roubados.
- Não conecte dispositivos de terceiros aos seus próprios dispositivos (*laptop*, *pen drive*, *MP3 player*, cabo de carregamento USB etc).
- Nunca use *pen drives* que tenham sido presenteados a você durante viagens (feiras, reuniões etc) ou que tenha encontrado em algum lugar. Eles podem conter programas maliciosos.

Se você lida com dados muito sensíveis, tem motivos para acreditar que pode ser alvo de espionagem empresarial ou industrial, ou viaja para países conhecidos por violarem os direitos civis, você deve considerar outras medidas:

Antes da viagem

- Use apenas dispositivos (computadores, mídias removíveis, telefone) designados para uso específico e que contenham apenas os dados necessários.
- Apague o histórico de chamadas e do navegador.
- Rotule seus dispositivos para garantir que não sejam trocados inadvertidamente.
- Se precisar acessar os sistemas de informação da empresa remotamente, instale um *software* VPN para proteger sua comunicação. Pergunte-se se realmente não consegue passar alguns dias sem acesso remoto a todos os seus dados empresariais.

Durante a viagem:

- Mantenha seus dispositivos, mídias de armazenamento e arquivos sempre com você durante a viagem e durante sua estadia (não os deixe em um cofre de hotel).
- Desligue seus dispositivos se precisar entregá-los em algum lugar. No caso de telefones e *smartphones*, remova também o cartão SIM.
- Informe sua empresa em caso de perda, roubo ou se seus dispositivos forem examinados ou confiscados por autoridades estrangeiras.
- Evite usar dispositivos oferecidos para uso durante a viagem e nunca insira senhas nesses dispositivos.

- Não conecte seu *hardware* a dispositivos nos quais você não confia. Se precisar trocar documentos durante uma apresentação de negócios, é melhor trocá-los por e-mail ou usar um *pen drive* específico para esse fim e, em seguida, excluir os dados usando um *software* de exclusão seguro. Ao carregar seu celular, evite conectá-lo a um computador não controlado ou a um carregador USB desconhecido (por exemplo, em aeroportos).

Após a viagem:

- Altere as senhas que você usou

Durante a viagem.

- Se possível, verifique seus dispositivos após a viagem. Caso contrário, adquira dispositivos adicionais e descarte-os após a viagem de trabalho.

Pergunta 11: Como você se informa e informa seus funcionários?

Informem-se e informe a seus funcionários

Tome precauções. As informações atuais sobre vulnerabilidades de *software* são publicadas nos chamados "*Security Advisories*". Deve-se verificar regularmente (ou seja, semanalmente) se o *software* ou *hardware* da sua empresa foi afetado e as recomendações de ação devem ser implementadas.

Como regra geral, é suficiente atualizar o sistema afetado. Como atualmente não há nenhum *Security Advisory* disponível nas instituições oficiais brasileiras, recomendamos que você se mantenha atualizado por meio de canais internacionais, como o CERT-EU[10].

Além disso, é recomendável que MPEs criem uma cultura de "higiene digital", informando regularmente aos funcionários sobre boas práticas de segurança e as principais ameaças que podem afetar as operações[11]. Uma carta ou um manual do setor de TI pode ajudar a promover essa conscientização.

Ela pode ser entregue a cada funcionário descrevendo as diretrizes para o uso adequado da TI e o processo de relato de incidentes. É importante relembrar a equipe da existência destes documentos com regularidades por meio de comunicações internas, em reuniões ou em um boletim informativo.

A promoção da notificação de incidentes de segurança de TI internos deve ser encorajada por meio de uma abordagem não punitiva. O objetivo é informar aos usuários de que as ameaças estão em constante evolução e despertar uma autoconsciência quanto à própria vulnerabilidade no ambiente digital. Somente assim é possível garantir que a maior quantidade possível de incidentes seja relatada.

Pergunta 12: Sua apólice de seguro também cobre riscos cibernéticos?

As seguradoras estão cada vez mais oferecendo produtos para auxiliar as empresas que são vítimas de *malware* ou ataques cibernéticos. Em caso de sinistro, o seguro oferece cobertura financeira para os danos e, frequentemente, assistência jurídica também. Em alguns casos, a seguradora ou um provedor de serviços por ela contratado pode até assumir as medidas de defesa contra um ataque cibernético iminente.

Existem diferentes tipos de cobertura, incluindo proteção contra roubo de identidade, garantias contra interrupção das operações comerciais, aconselhamento jurídico no caso de violações de proteção de dados pessoais e suporte técnico na restauração do sistema de informações após um ataque cibernético.

[10] *Security Advisory* do CERT-EU: https://cert.europa.eu/publications/security-advisories/2023

[11] Confira o Dica do Dia https://cartilha.cert.br/ e segue as canais do https://internetsegura.br/

As cláusulas de seguro podem ser incluídas em contratos de seguro tradicionais ou assumir a forma de uma apólice especializada em seguro cibernético. Esta ainda é muito recente no mercado de seguradoras e pode estar em fase de desenvolvimento em algumas empresas. De qualquer forma, é importante garantir que os riscos mais significativos para a continuidade da empresa estejam cobertos.

Pergunta 13: Você configurou um *firewall*?

Por que o *firewall* local deve ser ativado? E como proceder?

Firewall é um sistema de segurança de uma rede de computadores que monitora o tráfego da rede de acordo com um conjunto definido de regras de segurança. Esse *software*, que é instalado no computador do usuário (diferente de um *firewall* central), protege principalmente contra-ataques da Internet.

O *firewall* também dificulta ou impede as ações de um agente mal-intencionado que pode ter hackeado um dos computadores de trabalho da rede. Os invasores frequentemente tentam penetrar nos outros computadores para obter controle completo do sistema e, por fim, acessar os documentos dos usuários. A ativação do *firewall* dificulta esse movimento lateral.

Microempresas

Sem conhecimentos avançados de TI, a ativação do *firewall* pré-instalado no computador de trabalho e sua configuração padrão (que bloqueia todas as conexões de entrada) representa um primeiro nível de proteção.

O *firewall* local é uma função disponível na maioria dos sistemas operacionais. Os *firewalls* podem ser encontrados em conjuntos a *softwares* antivírus.

Pequenas e médias empresas

Um *firewall* local (integrado ao sistema operacional ou como solução de *software* de terceiros) deve ser instalado em todos os computadores de trabalho. Recomenda-se garantir configurações e políticas de filtro consistentes. Uma configuração de filtro rigorosa deve ser capaz de bloquear todas as conexões não essenciais e registrar as conexões bloqueadas.

Além disso, as MPEs também devem usar principalmente *firewalls* centralizados (ou seja, *hardware* especializado) para proteger a conexão entre o sistema de informação e a Internet. Empresas que desejam ser especialmente cuidadosas em relação à segurança e/ou possuem uma grande rede de TI devem dividir a rede corporativa em zonas com diferentes níveis de segurança de acordo com a vulnerabilidade às ameaças.

Quanto à conexão com a Internet, idealmente ela deve ser implementada por meio de uma zona desmilitarizada (DMZ), que consiste em *firewalls* e em serviços de *proxy*, especialmente para comunicação e navegação na Internet.

Pergunta 14: Você sabe como reagir a um ataque cibernético?

Na parte III desta cartilha, você encontrará um passo a passo detalhado de como elaborar um plano de "procedimento emergencial" para incidentes cibernéticos e como agir nestes casos. Aqui você encontrará um resumo dos principais pontos.

Prepare-se para um incidente

Micro, pequenas e médias empresas devem considerar que estão sempre vulneráveis a um incidente sério de segurança de TI e devem identificar com antecedência os provedores de serviços especializados no combate a incidentes de segurança.

Além disso, prepare um conceito de segurança e um plano de ação caso um incidente ocorra, indicando responsabilidades de gerenciamento de TI e de gerenciamento da empresa em estado emergencial. Também é recomendável um plano de comunicação com órgãos públicos, funcionários e outras partes interessadas.

O NIC.br (Núcleo de Informação e Coordenação do Ponto BR) opera o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). O CERT.br apoia o processo de recuperação e análise de sistemas comprometidos para todos os sites registrados no Brasil[12]. No site do CERT.br, você encontrará checklists de segurança e melhoras práticas[13].

No caso de um incidente comprovado

Em caso de incidente em um sistema de informação, o primeiro passo é desconectar da Internet os seus dispositivos ou o sistema de informação da sua empresa. Para dispositivos individuais, isso pode envolver desconectar o cabo de rede ou desativar os serviços de Wi-Fi. Para o sistema de informação de uma empresa, isso pode ser feito nos componentes de rede ou no *firewall* da empresa. Isso impede que o invasor controle o ataque, como no caso de ransomware, e evita a possível extração de dados.

Atenção: não desligue nem altere os computadores e dispositivos afetados pelo ataque para não atrapalhar o trabalho dos investigadores/forenses de TI envolvidos.

Se um resgate for exigido, nunca ceda às demandas. Primeiramente, não há garantia de que você realmente receberá a chave de descriptografia após pagar o resgate. Em segundo lugar, você ainda precisa descobrir como os invasores obtiveram acesso ao seu sistema e fechar essa porta de entrada. Caso contrário, seus dados podem ser criptografados novamente. Lembre-se: quem paga uma vez, paga duas vezes!.

Além disso, após ler a pergunta 4 desta cartilha, você já se certificou de que todos os seus dados importantes estão protegidos. Embora as vítimas de ataques de *ransomware* frequentemente enfrentem o problema de ter seus dados extraídos/roubados antes da criptografia, caso a empresa tenha *backup* disponível, pode restaurar os dados após fechar o ponto de entrada utilizado pelos invasores e retomar as operações comerciais normais.

Recomenda-se a criação de um livro de registro para acompanhar as ações e os eventos relacionados ao incidente. Cada entrada nesse documento deve conter pelo menos as seguintes informações: a hora e a data da ação e do evento, o nome da pessoa que tomou a ação ou foi informada do evento e a descrição da ação ou do evento. Um livro de registro atualizado regularmente durante todo o incidente facilita consideravelmente a intervenção do provedor de serviços e a resolução do problema.

Além disso, é essencial que uma MPE desenvolva um conceito de comunicação interna e externa que possa ser implementado imediatamente no caso de um ataque. Além disso, os funcionários podem ser informados por meio da carta de TI, citada anteriormente, sobre como devem se comportar em caso de incidente comprovado.

Aspectos legais

As empresas que processam dados pessoais estão sujeitas ao Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) e devem cumprir os requisitos dessa legislação. Caso o incidente envolva dados pessoais, as empresas devem informar aos controladores de dados da empresa, os seus clientes, os titulares dos dados e, ainda, a Autoridade Nacional de Proteção de Dados.

[12] Para entrar em contato com o CERT.br envie um e-mail para: CERT.br <cert@cert.br>
[13] https://www.cert.br/links/#checklists

Pergunta 15: Você treina para a emergência?

A prática leva à perfeição!

Depois de criar um conceito de segurança e um plano de ação frente a ataques cibernéticos, a emergência deve ser praticada regularmente. Reserve tempo suficiente para executar uma simulação: desde a descoberta do ataque, medidas técnicas para contê-lo, notificação e cooperação com as autoridades, até a comunicação com a mídia e negociação com os criminosos.

Todas as pessoas da empresa sabem exatamente quais são suas respectivas funções e como agir em caso de incidente?

Há uma equipe de crise predefinida que lida com o gerenciamento do ataque e tem as competências necessárias para agir rapidamente? Quais provedores de serviços e autoridades podem ajudá-lo a lidar com o ataque? Quais autoridades você precisa notificar? É possível manter as operações, pelo menos parcialmente, talvez por meio de processamento analógico?

Responder a essas perguntas em teoria é um primeiro passo importante, mas sem a prática regular, há um alto risco de cometer erros no calor do momento ou perder um tempo valioso devido a responsabilidades e processos pouco claros.

Para tornar o processo mais fidedigno e educativo, existem fornecedores especializados que simulam ataques cibernéticos com sua empresa.

Não se intimide com o esforço supostamente grande de tirar os tomadores de decisão da atividade operacional por um dia. Se um ataque cibernético afetar sua empresa durante vários dias ou até semanas, o prejuízo será muito maior.

Parte III

Parte III: Gerenciamento de incidentes e recuperação

Um ataque cibernético influenciará negativamente suas operações e você não poderá prestar os serviços aos seus clientes de forma adequada. Isso significa redução ou ausência de receita durante esse período.

Um ataque completo que compromete todo o seu sistema pode levar a um tempo de inatividade da sua empresa de 2 a 4 semanas. Você sabe como ninguém o que isso pode significar financeiramente para sua empresa.

Portanto, é essencial ter um bom plano de como agir em caso de ataque cibernético. Estabeleça um gerenciamento de crise adequado que, além dos aspectos técnicos de recuperação (sessão 1), aborde medidas organizacionais, especialmente a comunicação com partes interessadas, autoridades e, se necessário, imprensa (comunicação de crise, sessão 1.3).

O conteúdo deste capítulo é baseado na publicação "Pronto Socorro em incidentes graves de TI" do Escritório Federal de Segurança da Informação (BSI) e foi validado por especialistas do setor privado do Brasil e da Alemanha.

É importante lembrar que cada ataque cibernético é um incidente grave e único e requer conhecimento especializado para ser resolvido. A depender da natureza do incidente, também são necessários avisos para as autoridades públicas responsáveis. Por isso, este guia visa sensibilizar empresas e demonstrar possíveis pontos a serem considerados durante um incidente.

De forma alguma, esta publicação objetiva ser um manual exaustivo para tratamento incidentes cibernéticos.

Medidas técnicas imediatas

Primeira regra: em nenhuma circunstância efetue um login com todas as contas de administrador em um sistema potencialmente infectado, enquanto o sistema ainda estiver conectado à sua rede produtiva interna ou à Internet!

Isole os sistemas potencialmente infectados da rede imediatamente para evitar a disseminação do *malware* por meio de movimento lateral. Para fazer isso, desconecte o cabo de rede. Não desligue o dispositivo. Se necessário, crie um *backup* forense, incluindo uma imagem de memória para análises posteriores (próprias, ou por terceiros) (consulte o ponto 3).

Gerenciamento de incidentes como um projeto

Se você não tiver experiência em lidar com incidentes graves de segurança de TI, talvez faça sentido encarar o gerenciamento de incidentes como um projeto e abordá-lo com ferramentas de gerenciamento de projetos.

O processo de gerenciamento de incidentes pode ser dividido em três fases, conforme descrito abaixo. Tente implementar essas medidas aos poucos na sua empresa.

Fase 1: Análise

- Identificação dos sistemas afetados;
- Prevenção de novas infecções e criptografia;
- Avaliação de danos;
- Análise do *malware*.

Fase 2: Operação de transição

- Prevenção de novas infecções e criptografia;
- Bloqueio do acesso dos criminosos;
- Monitoramento intensivo da rede.

Fase 3: Limpeza

- Concepção / implementação / reinicialização;
- Medidas de segurança adicionais (novo conceito de segurança).

O foco deste documento é ajudar as pessoas afetadas a terem um bom começo na fase 1.

Equipe de crise

Um ataque cibernético impactar seus serviços e produtos, sendo assim incidentes de segurança de TI exigem medidas administrativas e organizacionais, além de mecanismos de enfrentamento técnico-operacionais.

É aconselhável entender o gerenciamento de um incidente de segurança de TI como um projeto e fornecer uma equipe e recursos para este fim, implementando as medidas técnicas e organizacionais descritas abaixo:

As principais características dos mecanismos de enfrentamento administrativo-organizacionais são:

- Perspectiva interdisciplinar e em vários níveis;
- Tratamento de questões estratégicas e áreas temáticas;
- Conhecimento de processos críticos de negócios e sua avaliação em nível gerencial;
- Gerenciamento da comunicação interna e externa;
- Competências de ação e tomada de decisões de longo alcance.

Essas características podem ser consideradas pré-requisitos a serem cumpridos constantemente pela sua equipe de projeto e exigem automonitoramento contínuo para manter o alinhamento administrativo-organizacional.

Portanto, envolva os órgãos internos relevantes desde o estágio inicial na construção da equipe de crise, que idealmente deve conter:

- Nível gerencial, como chefe da equipe de crise (se possível, no entanto, não "o chefe" da instituição), para que a equipe de crise também tenha o apoio formal da gerência, mas que o líder da empresa não fique sobrecarregado.
- Gerenciamento de TI: ponto focal técnico da equipe de crise, mantém as forças operacionais livres para o trabalho.
- Advogados: lidam com questões sobre responsabilidade, acusações criminais e outros aspectos legais.
- Imprensa e relações públicas: fornecem a comunicação interna e externa adequada da crise, preserva a reputação da empresa, protegem as relações comerciais e motiva os funcionários.
- Oficiais de proteção de dados: lidam com questões de proteção de dados, como registro de incidentes.
- Recursos humanos: devido ao acesso aos dados de registro, devem lidar com questões relacionadas ao pessoal, como horas extras.
- Planeje fases regulares de consulta da equipe de crise alternadas com fases de trabalho

Não é necessário ter uma equipe do departamento de TI para todas as funções de gerenciamento de crises!

Os gerentes de projeto e os especialistas de escritório podem apoiar e aliviar os especialistas de TI em muitas tarefas organizacionais, de planejamento, de comunicação ou de logística. Se necessário, conte com o apoio de um gerente de crise externo experiente para ajudá-lo a lidar com o incidente.

Provavelmente, você terá que limpar o *Active Directory* (AD) em curto prazo e configurá-lo novamente em médio e longo prazo. Verifique se os ADs não afetados e os *backups* (parciais) estão disponíveis em outros locais ou em partes remotas/separadas da empresa.

No curto prazo, crie um grupo de projeto que, em paralelo às suas análises e contenções, inicie uma nova configuração de rede, especialmente para processos comerciais críticos para manutenção ou restauração da produção em área segmentada (com suporte externo, se necessário).

Cuide dos seus colegas que estão trabalhando com desempenho máximo para lidar com a situação. Ofereça boas condições de trabalho (bebidas, lanches, uso de táxi e, se necessário, hotel em vez de uma longa viagem de carro para casa).

Fique atento aos sinais de sobrecarga e faça planejamento de plantões ou turnos adequados para a situação de crise para que eles possam se acalmar novamente e recarregar as baterias. Tenha em mente que tudo o que você faz pelos seus colegas é mais econômico do que uma perda prolongada de produção devido a erros ou sobrecarga!

Mas pense também nos funcionários que podem trabalhar pouco ou nada devido a falhas de TI. Tente encontrar um trabalho significativo para eles e estabeleça uma operação de emergência.

Esses funcionários também podem ainda ter dados armazenados localmente e auxílios de trabalho (possivelmente contrários às diretrizes da empresa). Com uma nota "não será punido", você ainda poderá encontrar dados valiosos aqui.

Comunicação

A comunicação, interna ou externa, em caso de incidentes graves de segurança de TI é uma das ferramentas mais importantes para o gerenciamento. Se o incidente tiver visibilidade externa, o desafio é ainda maior. Portanto, essa área temática deve receber uma importância especial.

Deixe a comunicação para os especialistas!

Se a sua empresa tiver recursos adequados próprios, como uma equipe de comunicação corporativa, é importante envolvê-los na equipe de crise/equipe de projeto o mais cedo possível. Se não for possível fornecer recursos adequados dentro de sua própria instituição, chame especialistas em comunicação externa. Depois de analisar a situação, eles irão sugerir medidas adequadas.

Forneça a infraestrutura de comunicação necessária!

Dependendo da extensão do incidente de segurança, a infraestrutura de comunicação existente, como os computadores com Internet e telefonia (VoIP) etc, pode não estar mais operacional. Portanto, forneça uma infraestrutura substituta adequada (*laptops* com *hotspot* móvel, telefones celulares com fones de ouvido) para as unidades envolvidas na comunicação assim que possível.

Identifique as partes interessadas e chegue a um acordo quanto às diretrizes de comunicação!

Para uma comunicação de crise adequada, você precisa saber quem serão as partes interessadas (receptores) da sua mensagem. Sua própria equipe, clientes, acionistas, fornecedores, órgãos reguladores e o público em geral são algumas das possíveis partes interessadas.

Ao se comunicar diretamente com as partes interessadas, você também pode abordar questões mais específicas que comumente preocupam aquele grupo, por exemplo, se há risco para terceiros (por exemplo, seus fornecedores ou clientes) por meio de conexões VPN que possam estar em vigor.

Estabeleça as diretrizes de comunicação em conjunto idioma com os departamentos da empresa envolvidos, e comunique-as dentro da instituição para que todos os participantes se adaptem de maneira ágil.

Comunicação interna antes da comunicação externa!

Pense em informar seus funcionários primeiro e informe-os prontamente sobre o histórico do incidente para evitar especulações. Dê instruções sobre como lidar com a imprensa e com as mídias sociais e conscientize os funcionários sobre as medidas que estão iminentes. As informações podem ser fornecidas por meio de avisos claramente visíveis, grupos de chat existentes ou pelo respectivo gerente. Envie pelo menos uma mensagem de "nós nos importamos". Não dizer nada não é uma opção recomendada!

Considere um comunicado à imprensa em um estágio inicial para obter o controle sobreas informações divulgadas e evitar especulações. É possível que as informações internas dos funcionários sejam divulgadas. Nesse caso, você deve estar pronto para falar. Use os meios de comunicação já conhecidos (sites, mídias sociais, etc) da sua instituição para direcionar as informações ao grupo-alvo.

Com o apoio dos representantes da equipe de crise e do encarregado de dados da empresa (se houver), informe imediatamente aos funcionários sobre a possibilidade de envolvimento pessoal, caso o uso de tecnologias e sistemas seja permitido para fins privados e os dados inseridos ou armazenados nesses sistemas infectados possam ter vazado.

Organize o fluxo de informações e use as perguntas frequentes!

Os canais que você usa para a comunicação de crises devem ser escolhidos com cuidado. Ao selecioná-los, leve em consideração os canais de informação conhecidos (endereços de e-mail centrais, números de telefone etc) e planeje o fluxo de informações de modo que:

- As informações de saída sejam enviadas, se possível, de um remetente central que não possa ser rastreado até uma pessoa e por meio do qual também se esperam reações/ consultas,
- Todos os canais de informação conhecidos externamente sejam monitorados,
- A equipe que recebe informações externas é adequadamente instruída e está apta a lidar com pessoas que fazem ligações enérgicas,
- Todas as informações recebidas podem ser reunidas em um local central para que eles possam obter rapidamente o panorama completo,
- As perguntas recorrentes e as mensagens relevantes da instituição são resumidas em um FAQ e publicadas adequadamente.

Não há lugar para acusações em uma crise!

A comunicação de crise não deve ser usada para culpabilizar ou punir os supostos criminosos. Uma comunicação de crise profissional e efetiva é a figura central da instituição em um incidente grave de segurança de TI e, possivelmente, a única maneira de criar uma percepção positiva. Portanto, aplica-se o seguinte:

- Não aponte o dedo!
- Somente mencione os nomes (da empresa) de terceiros envolvidos (por exemplo, prestadores de serviços de TI) após consulta;

- Encoraje a colaboração cooperativa entre todas as partes envolvidas com o objetivo comum de gerenciamento amplo;

- Diga a verdade publicamente a seus funcionários o tempo todo.

Restauração de curto prazo da capacidade de trabalho

A restauração da operacionalidade total exige que o *Active Directory (AD)* afetado seja reiniciado regularmente. Para a restauração de curto prazo de uma capacidade de trabalho parcial, é aconselhável primeiramente atribuir cada serviço a uma das quatro categorias a seguir.

- **"Não afetado"**

Serviços que não usam nenhum dos sistemas afetados.

- ***"Offloadable"* (Terceirizável)**

Serviços que usam os sistemas afetados, mas podem ser terceirizados para outro sistema próprio ou de terceiros. A capacidade de terceirização pode variar muito, dependendo dos serviços, mas principalmente do tamanho da organização, do ambiente organizacional e de seu próprio cenário de AD.

Essa categoria inclui serviços para os quais outras áreas da empresa ou outras empresas próximas (por exemplo, outra empresa do grupo, município vizinho, escritório de uma associação) podem fornecer equipamentos de TI necessários aos funcionários por um curto prazo.

- **"Capacidade de trabalho pelo menos limitada com equipamento móvel"**

Serviços que usam sistemas afetados, mas que também podem ser fornecidos por meio de equipamentos móveis não afetados (*laptop* "limpo", ponto de acesso móvel, telefone celular), ainda que de forma limitada.

Diferentemente dos serviços que podem ser terceirizados, os serviços desta categoria são aqueles cujos *softwares* utilizados funcionam puramente no lado do cliente ou o componente do servidor externo pode ser acessado pela Internet.

- **"Impossível de trabalhar sem reconstrução"**

Serviços para os quais a capacidade de trabalho não existe ou não pode ser estabelecida de acordo com as categorias mencionadas acima.

Em uma próxima etapa, entre os serviços de cada categoria, podem ser identificados aqueles que são considerados funcionalmente importantes e que, portanto, precisam ser tornados operáveis de forma prioritária.

Análise de danos

O gerenciamento de danos exige uma análise precisa de quais são danos envolvidos. Além do conhecimento obtido durante a categorização no capítulo anterior, é necessário criar uma visão geral dos dados existentes (sistemas não afetados, *backups*), bem como dos dados a serem obtidos de fontes de dados externas.

Além de avaliar o dano, é necessário desvendar a sua causa. Isso garantirá que as vulnerabilidades responsáveis pelo incidente de segurança possam ser eliminadas.

Vazamento de dados

Atualmente, é comum que os invasores copiem dados durante um ataque de *ransomware* e depois ameacem publicá-los. Portanto, a página de vazamento deve ser monitorada quanto a isso. Se os dados do incidente forem publicados, eles devem ser analisados e os afetados devem ser informados sobre os fatos e o risco que surgiu.

Suporte externo

Muitas vezes, as empresas afetadas não têm experiência ou recursos internos suficientes para lidar com sucesso com incidentes graves de segurança de TI. Para muitas das pessoas afetadas, é a primeira vez que elas são confrontadas com um incidente de segurança grave nesta área.

Portanto, entre em contato com especialistas externos assim que você se sentir sobrecarregado ou confuso quanto aos próximos passos.

As recomendações a seguir com relação ao suporte externo se aplicam às instituições no Brasil. Em outros países, as autoridades locais relevantes devem ser contatadas.

Provedor de serviços de segurança de TI

Em geral, ao escolher uma empresa forense, deve-se observar que as empresas têm diferentes focos de análise. O espectro de especialização varia desde a análise de ataques baseados em rede até a recuperação de discos rígidos fisicamente destruídos. Os provedores de serviços qualificados estão preparados para reagir rapidamente.

A necessidade de suporte deve ser descrita da forma mais clara possível na solicitação. Você precisa de ajuda para limpar os sistemas e o AD, caso o vetor de ataque seja encontrado, ou outros sistemas afetados? É necessária uma equipe para reconstruir a rede?

Associações

Se você for membro de uma associação, talvez consiga obter apoio por meio dela. Se necessário, use suas redes profissionais para obter ajuda, reforço de pessoal, alívio, assumir serviços parciais como alternativa temporária, etc.

O NIC.br (Núcleo de Informação e Coordenação do Ponto BR) opera o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). O CERT.br apoia o processo de recuperação e análise de sistemas comprometidos para todos os sites registrados no Brasil.

Polícia

O Artigo 154-A do Código Penal Brasileiro prevê multa e reclusão de 1 a 4 anos em caso de ataque a sistemas de TI, prevendo ainda circunstâncias agravantes ao crime. Em caso de invasão que resulta em prejuízo econômico a pena pode aumentar em um ou dois terços. Em caso de obtenção de conteúdos sigilosos conforme definidos em Lei, como segredos comerciais ou industriais e obtenção de conteúdo de comunicações eletrônicas privadas, a reclusão aumenta para 2 a 5 anos.

Em princípio, recomenda-se registrar uma queixa criminal na Polícia Civil para quaisquer ataques cibernéticos sofridos. Em alguns estados, a Política Civil possui delegacias especiais para esse tema. Caso não haja uma por perto, a delegacia de polícia mais próxima pode entrar em contato com divisão especial do estado para solucionar o caso[14]. Os agentes também fornecem informações do que fazer e podem auxiliar na investigação do ataque.

Pagar um resgate?

Caso a criptografia já tenha sido realizada, a recomendação é que você geralmente não deve responder a nenhuma forma de extorsão e não deve pagar um resgate. Em vez disso, os dados devem ser restaurados após a limpeza da rede a partir de *backups* existentes com integridade.

No entanto, se os *backups* também tiverem sido criptografados e, portanto, estiver sendo considerada uma tentativa de obter uma chave para descriptografar os dados pagando o resgate, lembre-se do seguinte:

[14] Delegacias Cibercrimes | SaferNet Brasil

- Se você tiver um seguro cibernético, informe-o logo no início. Eles geralmente darão instruções sobre o que você precisa fazer para que eles paguem por quaisquer custos incorridos.

- Ao pagar um resgate, você pode estar financiando outros ataques a terceiros. Certifique-se de esclarecer quaisquer pagamentos com as autoridades de investigação relevantes ou com seu departamento jurídico/advogados.

- Em alguns casos, o valor do resgate pode ser significativamente reduzido em negociações profissionais por provedores de serviços de segurança de TI.

- Apesar do pagamento, você não tem nenhuma garantia de que realmente receberá uma chave adequada, afinal, você está negociando com criminosos.

- Algumas das chaves recebidas podem não ser adequadas para seus dados ou a rotina de criptografia pode estar com defeito. Portanto, no início das negociações, peça aos criminosos que descriptografem alguns arquivos, por exemplo, para verificar se eles estão de posse da chave correta em primeiro lugar.

- A descriptografia bem-sucedida não substitui a reinstalação dos sistemas comprometidos. Para excluir o acesso adicional dos perpetradores à rede interna e impedir a disseminação renovada do *malware*, é imperativo que seja feito o *backup* de todos os dados após a descriptografia e que eles sejam restaurados depois que a rede for reconstruída. Isso é especialmente importante porque os criminosos podem ter deixado um *backdoor* para trás, o que pode levar a uma nova criptografia - afinal, você já pagou uma vez, então por que não pagaria novamente?

Se você pagar o resgate mesmo assim, contrariando a recomendação, informe a polícia. Se necessário, eles poderão rastrear o fluxo de dinheiro e identificar os criminosos.

Obrigações legais e contratuais

Você deve considerar ainda todas as obrigações de comunicação aos órgãos governamentais, como agências reguladores, por exemplo, de acordo com a LGPD e outras leis vigentes no Brasil.

Mesmo que um ataque seja descoberto relativamente cedo, há uma grande probabilidade de que os dados em que o invasor tem interesse e aos quais ele tem acesso já tenham sido vazados. Por exemplo, o *malware* "Emotet" espiona as caixas de correio do Outlook e roteia automaticamente os contatos e os conteúdos dos e-mails.

Em caso de violações à LGPD, como vazamento de dados pessoais - o que sempre acontece, por exemplo, em infecções por "Emotet", é obrigatório notificar o ocorrido à Autoridade Nacional de Proteção de Dados (ANPD), enquanto autoridade responsável sobre o tema, e também aos titulares dos dados, conforme previsto no Artigo 48 da LGPD. Esse processo pode ser realizado por meio do preenchimento de formulário, que deve ser protocolado por meio do Peticionamento Eletrônico do SUPER.BR.

Em caso de dúvidas a respeito do procedimento de comunicação de incidentes de segurança, a Coordenação-Geral de Fiscalização (CGF) da ANPD pode ser acionada pelo e-mail: fiscalizacao@anpd.gov.br. A ANPD recomenda enviar o formulário informando o vazamento em até 2 dias úteis da ciência do fato.

Além de obrigações previstas na LGPD, pode haver obrigações de informar seus parceiros decorrentes de eventuais contratos que você tenha celebrado. Se você tiver contratado uma apólice de seguro cibernético, informe-a em um estágio inicial. Eles geralmente lhe darão instruções sobre o que você pode fazer.

Acompanhamento

Após o incidente de segurança, tire um momento para avaliar coletivamente o ocorrido e pensar em sugestões de aprimoramento. Tente responder às seguintes perguntas:

- Que medidas de longo prazo precisam ser tomadas?
- O que deu certo e onde há potencial para melhorias?
- Onde as medidas de segurança devem ser aprimoradas?

Planeje uma auditoria externa da sua TI depois que as medidas forem implementadas. Talvez associações ou empresas de TI da sua região já possuam uma lista de provedores de serviços de segurança de TI certificados nas áreas de auditoria e teste de penetração de sistemas operacionais. Além disso, estes servidores podem oferecer outros serviços relevantes para o seu caso.

Agradeça aos seus contratados e clientes pela compreensão, paciência e apoio. Com alguma distância, planeje um "agradecimento" para a sua equipe envolvida na resposta a incidentes. Use suas opções de bônus, licença especial, festa de encerramento, etc. Mesmo esse "pequeno investimento" será compensado a longo prazo!

International Digital Dialogues

Shaping digital policy together