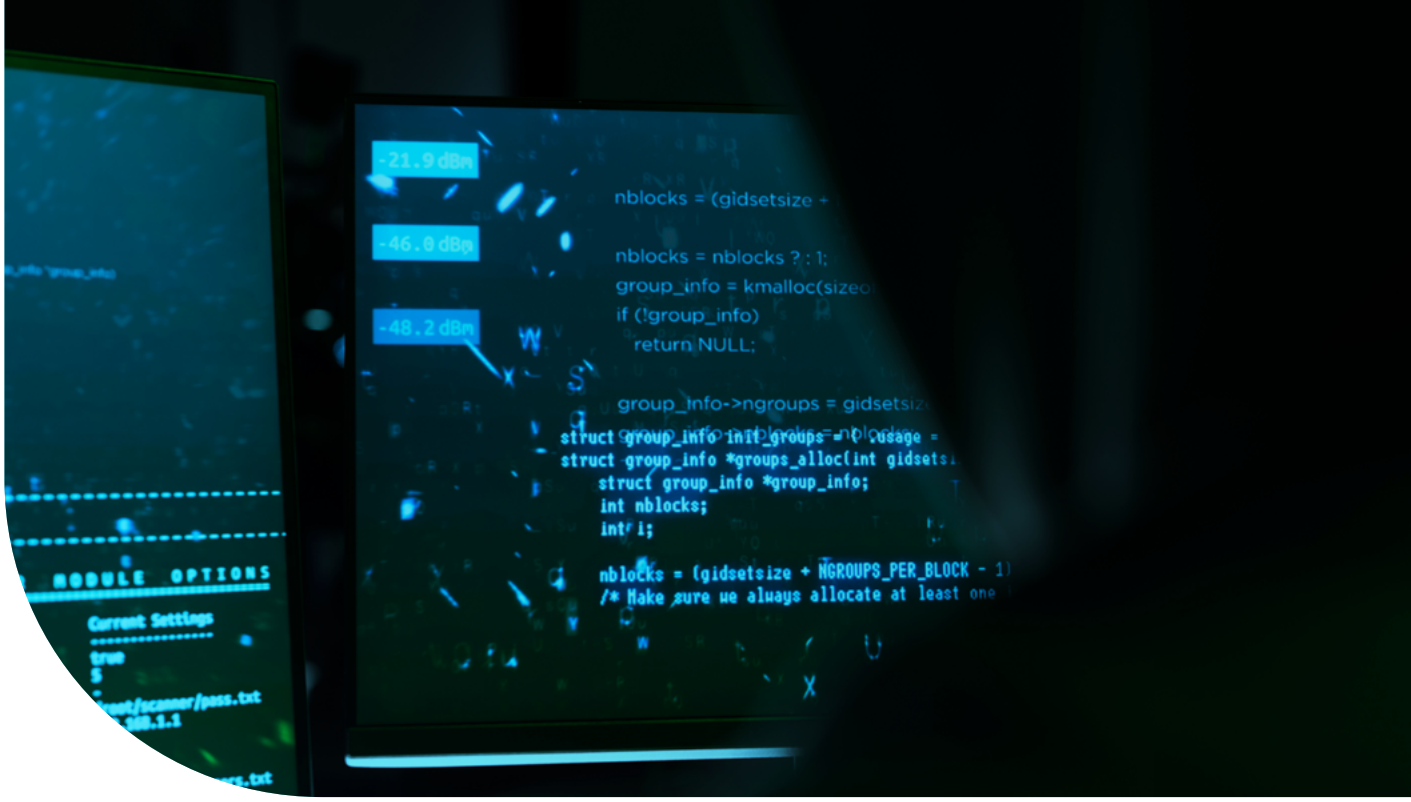
PLANO DE CONTINGÊNCIA EM TI

Como se preparar para um ataque cibernético

Digital Security
Progress. Protected.



De uma hora para outra, todos os dispositivos entram em modo de suspensão, o site fica fora do ar e ninguém da sua equipe consegue acesso à rede ou aos dados. Há uma repentina paralisação em toda a área de TI. O tempo passa e a situação permanece assim pelas próximas quatro semanas, pois a empresa não está preparada para esse tipo de incidente. Muitas organizações, especialmente as de pequeno e médio porte, não têm uma preparação para esse tipo de ataque, causado por cibercriminosos. Quais atitudes tomar frente a um ataque cibernético?

Apesar do aumento no número de ataques cibernéticos nos últimos anos e da aceleração dessa tendência causada pela pandemia de covid-19, o assunto ainda é subestimado em grande parte das empresas. De acordo com a Momentive Q3 Small Business Survey da CNBC, de 2021, 56% dos proprietários de pequenas empresas dos Estados Unidos afirmaram não estarem preocupados em ser vítimas de um ataque hacker nos próximos

12 meses, e 24% declararam não estarem “nem um pouco” preocupados. Além disso, apenas 28% das pequenas empresas afirmaram ter um plano pronto para resposta a um possível ataque cibernético, ao passo que 42% declararam não ter plano algum e 11% revelaram “não ter certeza” da existência de um plano em suas empresas.

13%

Porcentagem de pequenas empresas que treinam sua equipe em segurança cibernética. Apenas 19% realizaram testes para avaliar as respostas da sua equipe, como simulações de phishing.

Fonte: pesquisa do instituto Ipsos Mori e Departamento de Cultura, Mídia e Esportes do governo do Reino Unido, 2021.

Especialistas avaliam esse comportamento como negligência. Os ataques cibernéticos não são mais uma possibilidade remota, mas uma realidade iminente. Essa perspectiva foi confirmada por uma pesquisa publicada em 2021, pela associação digital alemã Bitkom.

Nove em cada dez

Quase 90% das mil empresas de todos os setores pesquisadas na Alemanha relataram terem sofrido ataques cibernéticos. Tipos de ataques mencionados com maior frequência:

86%

das empresas tiveram prejuízos causados por um ataque cibernético. Em 2019, esse número era de apenas de 70%

Fonte: Pesquisa da Bitkom, na Alemanha, comparação de pesquisas realizadas em 2019 e 2021

Iniciando um plano de contingência eficaz

Especialistas em medicina de emergência chamam a fase decisiva de lesões ou doenças que ameaçam a vida de "hora de ouro" Quanto mais rápida for a resposta, maiores serão chances de uma recuperação completa. A gestão profissional de continuidade de negócios é um pré-requisito para uma hora de ouro bem-sucedida em um contexto operacional. **O objetivo é aumentar a confiabilidade dos processos e responder rápida e sistematicamente em caso de emergência**, especialmente em caso de ataques de hackers e malware.

O plano de contingência, também conhecido como gerenciamento de incidentes em TI, costuma abranger todo o processo organizacional e técnico para a reposta a incidentes de segurança detectados, suspeitos ou falhas nas áreas de TI, bem como medidas e processos preparatórios. O espectro de possíveis incidentes varia de problemas técnicos e pontos fracos até ataques específicos à infraestrutura de TI. O gerenciamento de incidentes em TI, no sentido mais restrito, deve **considerar todos os detalhes organizacionais, legais e técnicos.**

As chances de cibercriminosos completarem um ataque com sucesso são diversas e bastante altas. Os cibercriminosos são altamente profissionais.

Atualmente, os cibercriminososstêm à disposição diferentes meios lucrativos de manipulação e disseminação de trojans, vírus e outros tipos de malware nas redes. Além disso, **um ataque cibernético nem sempre é identificado de forma imediata**, pois nem todos os níveis do sistema estão sob observação.

Uma boa preparação é fundamental para a criação de um plano de contingência. O motivo é que, caso ocorra o pior cenário, o mais importante é ter uma resposta rápida: interromper o ataque o mais rápido possível, proteger os dados armazenados e restaurar as operações normais da empresa o quanto antes.
Portanto, é necessário definir uma variedade de medidas imediatas: por

exemplo, quando toda a rede de comunicação do escritório entra em colapso, os sites ficam indisponíveis, ou mesmo todo o processo de produção fica paralisado após um ataque.

Como elaborar um plano de contingência:

- **Desenvolva um plano de contingência operacional:** Registre todas as medidas necessárias, que devem ser tomadas em caso de emergência. É indicado buscar o aconselhamento profissional de especialistas. Uma visão geral inicial também pode ser encontrada em modelos de amostra.
- **Nomeie um oficial de segurança cibernética:** indique uma pessoa responsável para lidar com questões de segurança na empresa. Desde a introdução do LGPD, as empresas com mais de dez funcionários devem nomear uma pessoa responsável pela proteção de dados.
- **Verifique seu plano de contingência atual:** caso já tenha um plano de contingência, deve ter sido verificado e implementado por especialistas. Também é necessário se certificar de que seu plano de contingência seja compreensível para leigos.
- **Prepare a sua empresa para todas as eventualidades:** para saber se o plano realmente funciona, é necessário realizar um teste prático.

Ataques cibernéticos: como lidar com o problema

Com o passar do tempo, os cibercriminosos vêm causando cada vez mais danos, infiltrando a arquitetura de TI até o menor elemento ou desviando dados extremamente confidenciais. Os gestores de TI têm, por conseguinte, a tarefa de reconhecer atividades prejudiciais em um estágio inicial, agindo de forma rápida. Essa é a única forma de reduzir efetivamente os danos causados e até mesmo evitar a falha total do sistema. Além das consequências financeiras, as empresas devem, acima de tudo, temer uma enorme perda de imagem e confiança por parte dos clientes. Então, como devem as empresas agir quando criminosos tomam posse dos dados corporativos e as comunicações do escritório ficam fora de ordem?

Onde buscar ajuda em caso de um ataque cibernético

- Revendedores de TI e fornecedores de sistemas têm ampla experiência com ataques cibernéticos e podem oferecer assistência rápida e direcionada.

- Caso seja possível em seu país, o incidente deve ser reportado. Por exemplo, no Reino Unido, é possível fazer a denúncia on-line à Action Fraud e, nos Estados Unidos, registrar uma ocorrência no site do FBI.

Nove dicas que vão te ajudar a minimizar o impacto de um ciberataque

1. Mantenha a calma e escolha a tática a ser usada

No caso de o software de segurança cibernética emitir um alerta, o primeiro passo é manter a calma. Um ataque cibernético bem-sucedido é, muitas vezes, uma surpresa. É possível que um malware se esconda na rede por semanas sem ser detectado, caso a TI falhe em monitorar todos os níveis do sistema. Porém, ao ocorrer um incidente, é importante tomar as decisões corretas no menor tempo possível. Sem um plano de contingência com medidas imediatas definidas, o caos pode ser efetivamente pré-programado.

2. Identifique a extensão da infecção

Muitos departamentos de TI de empresas que são vítimas de ataques de malware confiam em sua intuição no lugar de uma análise detalhada para determinar as consequências desses ataques. Naturalmente, é importante ter uma resposta – mas não com base em suposições. No caso de uma empresa com um plano de gerenciamento de emergências em TI funcionando, o departamento de TI pode rapidamente encontrar as respostas certas para questões centrais:

☑ Quais sistemas foram infectados?

☑ Como ocorreu o incidente?

☑ Foram perdidos dados importantes da empresa?

☑ A infecção está afetando apenas componentes individuais ou toda uma sub-rede?

☑ Os invasores tiveram acesso a informações de clientes e dados de funcionários?

3. Assegure o funcionamento das operações de TI

Caso pessoas não autorizadas tenham acesso às informações internas, a equipe e clientes afetados devem ser informados. Caso os sistemas de TI sejam gravemente afetados por um ataque, é necessário ativar os sistemas de backup e as conexões de rede redundantes, pois é fundamental que o negócio não sofra com o impacto do ataque cibernético. Para o garantir, é igualmente necessário um plano de contingência para reduzir os tempos de resposta.

4. Contenha a infecção

Os sistemas de TI infectados devem ser isolados. Para impedir a propagação da infecção na rede, o departamento de TI pode desconectar os segmentos de rede em que os dispositivos infectados estão localizados. Assim, os invasores não terão mais acesso a esses sistemas, sendo impedidos de "extrair" dados úteis.

De qualquer forma, o departamento de TI deve tentar decodificar o tráfego de dados criptografados entre os sistemas de TI infectados em sua própria rede e os computadores dos invasores. Assim, é possível determinar se houve a contaminação de outros dispositivos na rede e quais regras de firewall são necessárias para impedir o acesso não autorizado. Essas contramedidas podem ser implementadas de forma muito mais rápida e eficiente com o uso de uma solução de segurança cibernética pela empresa — como as novas soluções comerciais da ESET.

5. Proteja as evidências

As evidências dos incidentes devem ser mantidas a fim de que as autoridades responsáveis pela aplicação da lei possam tomar medidas após um ataque bem-sucedido. A documentação abrangente também pode auxiliar na solicitação de uma apólice de seguro cibernético, caso tenha um.

6. Elimine a infecção e previna novos ataques

Uma das tarefas mais complexas é remover o malware dos sistemas de TI afetados e evitar ataques futuros no mesmo formato. Uma ferramenta

comprovada é o software antivírus ou antimalware que limpa automaticamente os sistemas de TI. Para prevenir novos ataques do mesmo tipo, as brechas de segurança que permitiram essas atividades devem ser eliminadas. Para confirmar, é aconselhável analisar os pacotes de dados transportados pela rede. O tráfego deve ser investigado, especialmente quanto aos padrões de tráfego e comandos utilizados anteriormente pelos invasores.

Outras precauções de segurança incluem verificar as regras do firewall e alterar as senhas utilizadas pela equipe para fazer login na rede. É recomendável considerar uma análise mais profunda do ataque cibernético, porque, em muitos casos, os ataques individuais fazem parte de ameaças persistentes avançadas (APT). Tratam-se de ataques cibernéticos contínuos, complexos e direcionados a pequenas e médias empresas e suas equipes. Se gestores se tornarem alvos destes APTs, é possível assumir que novos ataques se seguirão.

7. Legislação – LGPD e outros regulamentos importantes

Após um ataque, surgem as questões legais, que devem estar elucidadas com antecedência. Desde a introdução do LGPD, certos incidentes devem ser comunicados às autoridades dentro de um determinado período. As obrigações legais de informação devem ser verificadas com antecedência junto ao seu departamento jurídico, a fim de que sua empresa permaneça em conformidade legal, evitando a necessidade de arcar com eventuais multas.

8. Não efetue pagamento em caso de ataque de ransomware

O software de extorsão é um meio popular de ataque realizado por cibercriminosos. O malware criptografa os dados das vítimas e os cibercriminosos exigem um resgate para os liberar. Nunca pague o resgate exigido – pois nunca há como ter certeza de que você receberá seus dados de volta. Além disso, ao pagar o resgate, você está apoiando esse modelo de financiamento de cibercriminosos e sinalizando sua disposição em pagar, o que pode ser interpretado como um convite para novos ataques.

.

9. Aprenda com os ataques cibernéticos e erros cometidos

É importante que as empresas aprendam com a análise dos ataques e adotem as precauções adequadas. Qualquer vulnerabilidade anteriormente desconhecida que tenha sido remediada apresenta, em última instância, uma oportunidade para aprimorar as medidas de defesa no perímetro da rede corporativa e fechar potenciais pontos de entrada. Também é crucial que gestores de TI mantenham a atenção a todos os níveis do sistema, facilitando a detecção de um ataque cibernético em estágio inicial, impedindo que os invasores tenham a oportunidade de imergir em áreas específicas e explorar o sistema antes de iniciar o próprio ataque.

Em caso de ataque cibernético, certifique-se de que:

- Nenhum dano adicional resulte do ataque.
- Medidas imediatas possam ser tomadas, independentemente de departamentos de hierarquia superior ou do nível executivo, para que não se perca tempo obtendo aprovação em caso de emergência.
- Dados de login possam ser alterados imediatamente. Senhas roubadas, logins e contas de e-mail contaminadas podem causar danos futuros. Por isso, seu plano de contingência deve incluir uma estratégia sobre como proceder após o ataque cibercriminoso com dados de acesso pertencentes à empresa.
- Mesmo os acessos de convidados, caso existam, sejam desativados e a rede desligada. Dispositivos de convidados não gerenciados representam, particularmente, um alto risco para a entrada de códigos maliciosos no sistema.
- Nenhum e-mail seja aberto, dispositivos móveis não sejam conectados à rede da empresa ou a outras redes, como redes de clientes, e todos os meios de armazenamento conectados à rede, como pendrives, discos rígidos externos, câmeras, entre outros, sejam desconectados e não utilizados nem removidos do local de trabalho.

Cinco dicas adicionais para uma segurança aprimorada

Ao seguir os passos listados acima, você já estará com uma ótima preparação para enfrentar um ataque. Aqui estão mais cinco recomendações que ajudarão a otimizar a segurança em sua empresa:

1. Automatize todas as etapas possíveis

No melhor cenário, o plano de emergência pode ser amplamente automatizado, utilizando ferramentas modernas. Todos os processos que podem ser executados de forma autônoma aliviam a carga do administrador. Essas ações podem incluir, por exemplo, o encapsulamento automático dos endpoints afetados, em que os firewalls do desktop cortam todas as conexões, exceto as de administração remota.

.

2. Preste atenção ao registro e à documentação

É igualmente importante que todas as ações, sejam automáticas ou manuais, incluam a documentação e o registro abrangente das etapas manuais. Somente dessa forma é possível rastrear o processo de infecção retrospectivamente e adaptar o plano de contingência de acordo – no que diz respeito ao fechamento de possíveis lacunas de segurança, mas também ao comportamento humano.

3. Faça backups com regularidade

Independentemente do que causou o incidente de segurança, a capacidade das empresas de recuperar dados comerciais importantes que foram perdidos o mais rapidamente possível é fundamental. O começo de tudo é a realização de backups regulares. Aqui, novamente, o backup automático de cópias de dados é uma boa escolha, pois garante a consistência das informações. Além disso, você evita que a equipe esqueça de fazer os backups. As cópias de backup devem ser realizadas em dois dispositivos externos, pelo menos. Além disso, deve-se considerar uma versão criptografada do backup armazenada em nuvem (considerando-se proteção de dados, de preferência em locais de armazenamento europeus). Novamente, os sistemas de backup e recuperação devem ser testados com regularidade.

4. Utilize uma ferramenta de detecção e resposta de endpoint (EDR)

Uma ferramenta EDR permite o monitoramento constante e abrangente de todas as atividades de endpoint. Dessa forma, os processos suspeitos podem ser analisados em detalhes e os gestores de TI podem responder a ameaças em sua fase inicial. Muitas vezes, as empresas reforçam suas medidas de segurança com o uso da tecnologia EDR, principalmente para casos de ataques de dia zero, ransomwares, ataques direcionados (APT) ou violações das políticas internas da empresa.

5. Reveja o seu plano de contingência com frequência

Assim como exercícios de simulação de incêndio, os planos de contingência em TI devem ser testados regularmente. Nada é mais fatal do que confiar em um plano que, no final, não funciona.

Conclusão

A contaminação de dispositivos, servidores ou sistemas móveis por softwares maliciosos pode representar uma ameaça séria para as organizações, especialmente quando os invasores conseguem acessar informações internas. No entanto, tais incidentes trazem à atenção dos responsáveis dois fatos importantes: por um lado, quais medidas de segurança cibernética precisam ser otimizadas e, por outro lado, o fato de que um sistema de contingência atualizado pode reduzir os danos.

Quando a tecnologia permite o progresso, a ESET garante a sua proteção

Há mais de 30 anos, a ESET® vem desenvolvendo softwares e serviços de cibersegurança líderes do setor para a proteção de empresas, infraestrutura essencial e consumidores em todo o mundo, contra ameaças digitais cada vez mais sofisticadas. De endpoint e segurança móvel à detecção e resposta de endpoint, bem como criptografia e autenticação multifator, as soluções de alto desempenho e fácil uso da ESET protegem e monitoram discretamente em tempo integral, com atualização das defesas em tempo real para manter os usuários seguros e os negócios funcionando sem interrupções. As ameaças em evolução requerem uma empresa de cibersegurança que evolui, permitindo o uso seguro da tecnologia. Contamos com o apoio dos centros de P&D da ESET em todo o mundo, trabalhando a serviço do nosso futuro compartilhado. Para mais informações acesse: eset-la.com ou nos siga no LinkedIn, **Facebook** y **Twitter**.

110 000 000+
de usuários protegidos em todo o mundo

300 000+
Novas amostras exclusivas de malware detectadas diariamente

600+
Especialistas em pesquisa e desenvolvimento

400 000+
Clientes empresariais em mais de 200 países e territórios