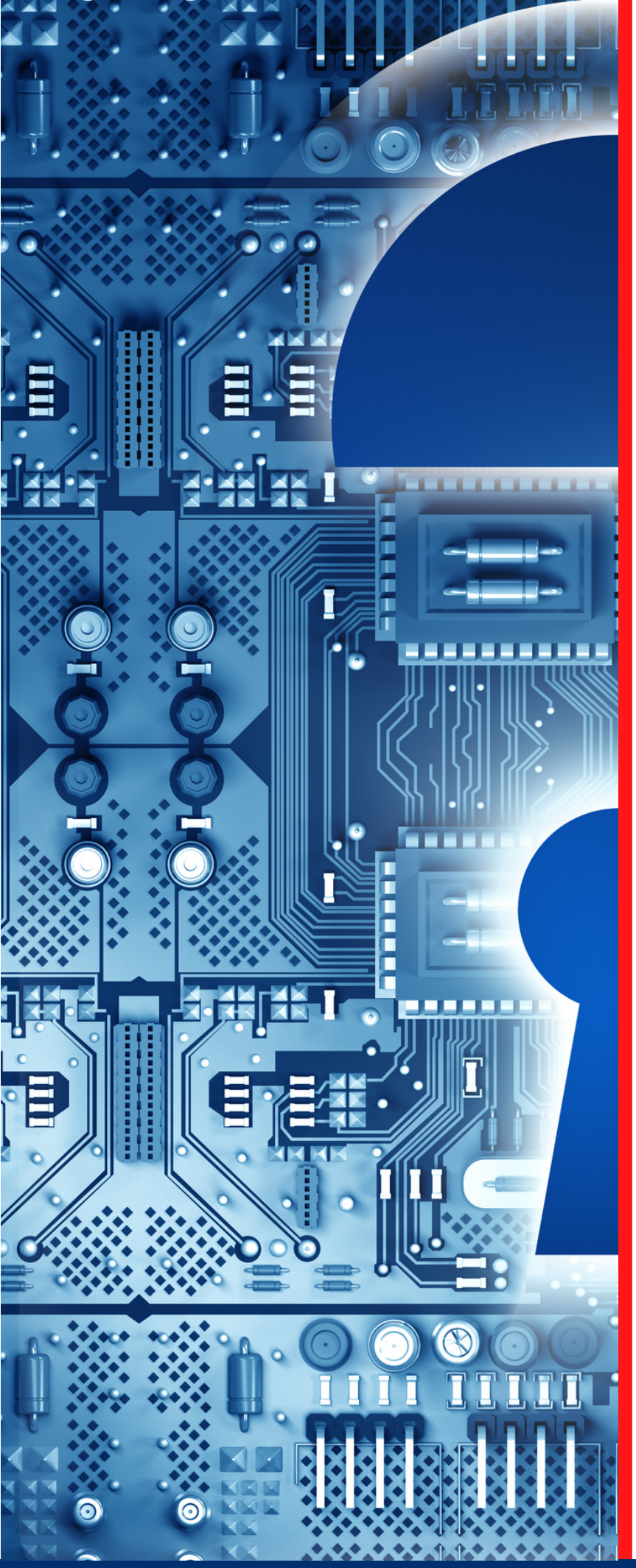


OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

12/2023

Ataques cibernéticos contra usuários em trabalho remoto

GOVERNO FEDERAL

BRASIL

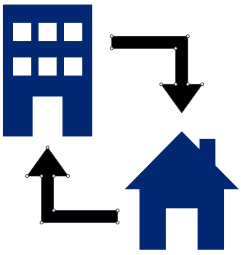
UNIÃO E RECONSTRUÇÃO

Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.

TLP:CLEAR

Motivação

Durante a pandemia da COVID-19, o trabalho remoto se popularizou no Brasil, particularmente por ser a principal maneira escolhida pelas empresas para manter suas equipes produtivas, mesmo com as limitações de um cenário de isolamento social.



Com o avanço tecnológico e o acesso à *internet* de alta velocidade, as empresas estão adotando maneiras de realizar as atividades profissionais sem a necessidade de estar fisicamente presente em um escritório ou local de trabalho convencional. Essa modalidade de trabalho, permite que os colaboradores executem suas tarefas de onde desejarem, desde que tenham acesso a uma conexão estável com a *internet*.

Contudo, o trabalho remoto também apresenta desafios. A conectividade com a rede da empresa e ferramentas para o acesso remoto podem ser alvos de ameaças cibernéticas. Manter o *Desktop* Remoto ativo em redes internas pode expor a organização a diversos riscos de segurança. Entender a tecnologia e aplicar boas práticas de prevenção permitirá que a instituição possa utilizar adequadamente essa ferramenta.

Tecnologias para trabalho remoto

A tecnologia de acesso remoto, também conhecida como *Remote Desktop*, é uma solução que permite aos usuários acessarem e controlarem um computador remotamente a partir de outro dispositivo. Essa solução é amplamente utilizada tanto por profissionais que trabalham remotamente quanto por equipes que precisam colaborar de diferentes locais de um país ou mesmo do mundo.

O principal benefício do uso do *Remote Desktop* é permitir que os usuários acessem e utilizem todos os recursos do computador remoto, incluindo aplicativos, arquivos e documentos. Isso oferece uma experiência semelhante à de estar fisicamente em frente ao computador, o que é útil quando se precisa trabalhar com programas ou arquivos específicos que não estão disponíveis fora da rede da instituição. Selecionamos a seguir cinco ferramentas de acesso remoto mais utilizadas e que estão disponíveis no mercado:

1. *TeamViewer*: Solução de acesso remoto amplamente utilizada por profissionais de TI. Este sistema permite o controle remoto de computadores, suporte técnico, transferência de arquivos e colaboração em equipe.

2. *AnyDesk*: Ferramenta que oferece uma conexão rápida e segura, com recursos avançados de transferência de arquivos, bate-papo e colaboração em equipe.

3. *Remote Desktop Protocol* (RDP): O RDP é uma tecnologia da *Microsoft* que permite aos usuários acessarem e controlarem remotamente computadores com sistemas operacionais *Windows*. É amplamente utilizado em ambientes corporativos e oferece recursos avançados de segurança.

4. *Virtual Network Computing* (VNC): Tecnologia que permite o acesso remoto a computadores por meio de uma interface gráfica. Existem várias implementações do VNC disponíveis, como o RealVNC, o UltraVNC e o TightVNC.

5. *Chrome Remote Desktop*: Extensão do navegador *Google Chrome* que permite o acesso remoto a computadores a partir de qualquer dispositivo com o *Chrome* instalado. É uma opção prática e fácil de usar, especialmente para profissionais que já utilizam o navegador *Chrome* regularmente.

Cabe destacar que o Protocolo de *Desktop* Remoto (RDP), citado anteriormente, é amplamente utilizado por administradores de rede como ferramenta para o gerenciamento de sistemas *Windows* e a prestação remota de suporte ao usuário na resolução de problemas. Recordamos, que os administradores possuem credenciais privilegiadas, que são alvos de grande interesse das ameaças. Uma vez vazadas estas credenciais têm grande potencial de comprometimento aos sistemas.

Ataques Cibernéticos contra *Remote Desktop*

Phishing: vetor comum de ataque cibernético no qual os *hackers* tentam obter informações, como senhas e dados de *login*, por meio de *e-mail*, mensagens de texto ou *sites* falsos. Os usuários podem ser enganados a clicar em *links* maliciosos ou fornecer suas credenciais sem perceber.

Malware: ampla gama de ameaças, como vírus, *worms*, *trojans* ou *ransomware*. Esses códigos maliciosos podem infectar dispositivos remotos e comprometer a segurança. Os usuários podem ser infectados ao baixar arquivos ou clicar em *links* suspeitos.

Brute Force: Nesse tipo de ataque, os invasores tentam adivinhar senhas e combinações de *login* para obter acesso não autorizado. Isso pode ser feito usando *scripts* que testam várias combinações automaticamente.

Ataque de negação de serviço (DoS): ataque que visa sobrecarregar os recursos de uma rede, serviço ou aplicativo remoto, tornando-os inacessíveis para os usuários legítimos. Isso é feito através do envio de um volume massivo de tráfego para o alvo.

Ataques de injeção de comandos: os invasores podem injetar comandos maliciosos ou manipulados para executar ações indesejadas nos servidores ou dispositivos de destino.

Ataques *Man-in-the-Middle* (MITM): representam uma ameaça significativa para os usuários de tecnologias de *Desktop* Remoto. Nesse ataque a ameaça intercepta o tráfego entre usuário e dispositivo remoto. Com isso, o atacante é capaz de monitorar, modificar e injetar dados maliciosos.

Ataques *Man-in-the-Middle* (MITM): representam uma ameaça significativa para os usuários de tecnologias de *Desktop* Remoto. Nesse ataque a ameaça intercepta o tráfego entre usuário e dispositivo remoto. Com isso, o atacante é capaz de monitorar, modificar e injetar dados maliciosos.

Sequestro de Sessão de Acesso Remoto: o invasor ganha acesso não autorizado a uma sessão de *Desktop* Remoto, normalmente retomando uma sessão legítima, a partir da exploração de vulnerabilidades da tecnologia empregada para o acesso remoto. Alguns *malwares* realizam a enumeração das sessões de *Desktop* Remoto para sequestrar estas sessões.

- Os ataques contra *Remote Desktop* são, por vezes, precedidos de varreduras em portas para identificar vulnerabilidades. As Portas são canais de comunicação que permitem a troca de informações entre dispositivos em uma rede. Cada porta está associada a um número específico e pode ser usada para diferentes serviços ou protocolos.
- As explorações de vulnerabilidades a partir de portas não se limitam a portas específicas. Os atacantes podem realizar varreduras em várias portas em busca de qualquer serviço vulnerável. Além disso, a exploração pode ocorrer em diferentes camadas do modelo OSI, desde a camada de aplicação até a camada de transporte.

Prevenção

A visualização e interação com servidores ou dispositivos por meio das tecnologias de acesso remoto é totalmente fatível. Neste caso, a tela do dispositivo remoto é transmitida para a máquina do usuário remoto, permitindo a visualização e o controle do sistema.

Com isso, várias vulnerabilidades podem ser exploradas inclusive a execução remota de código (RCE), como a CVE-2022-21893, de alta severidade e específica na execução de código usando o RDP.

As ferramentas de acesso remoto não são Redes Privadas Virtuais (VPNs). A preocupação principal é com a funcionalidade e não com a segurança. Portanto, cabe ao usuário se precaver quanto às ameaças. Algumas medidas preventivas recomendadas são:

- Utilizar autenticação em múltiplos fatores (MFA): implementar autenticação em vários fatores é uma camada adicional de segurança que exige, pelo menos, um segundo método de verificação além das credenciais de *login* padrão. Isso ajuda a proteger contra os ataques de força bruta e previne o acesso não autorizado mesmo se as credenciais forem comprometidas.

- Configurar o acesso seguro: permitir o acesso remoto apenas por meio de conexões seguras. Isso inclui a utilização de conexões criptografadas (por exemplo, protocolo TLS) e a desativação de criptografia fraca ou desatualizada. Evite exposição diretamente à *Internet*, utilizando VPNs para acessá-lo de forma remota.

- Manter os sistemas atualizados: mantenha os sistemas atualizados com as últimas correções de segurança, inclusive navegadores e sistema operacional, tanto no servidor quanto nos dispositivos de acesso remoto.

- Fortalecer as senhas: use senhas fortes e complexas para contas de acesso remoto. As senhas devem ter comprimento suficiente, incluir uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Evite senhas óbvias ou fáceis de adivinhar.

- Limitar tentativas de *login*: configure restrições para limitar o número de tentativas de *login*, bloqueando temporariamente o IP ou conta após várias tentativas malsucedidas.

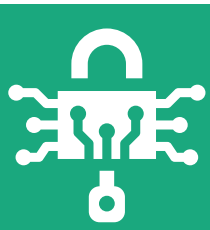
- Atualizar os ativos de segurança: aplicar *patches* de segurança, atualizar sistemas, fortalecer configurações de autenticação e implementar soluções de segurança adicionais e atualizadas, como *firewalls*, sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS).

- Uso de certificados digitais: solução para autenticar o servidor de acesso remoto prevenindo ataques de interceptação ou falsificação. Certificados digitais são emitidos por Autoridades de Certificação e permitem a autenticação e a criptografia da comunicação, possibilitando a confidencialidade e integridade dos dados transmitidos entre o usuário e o servidor remoto.

- Atualizar a tecnologia de acesso remoto utilizada: aplicação regular de *patches* e atualizações de segurança para mitigar vulnerabilidades conhecidas e a restrição de acesso a sessões de acesso remoto.

- Habilitar o *Network Level Authentication* (NLA): camada adicional de segurança ao processo de conexão remota, exigindo que autenticação antes que a sessão seja estabelecida. Isso significa que as credenciais de autenticação são verificadas antes mesmo de permitir o acesso.

- Usar criptografia: recomenda-se o uso de algoritmos de criptografia robustos, como AES (*Advanced Encryption Standard*), que oferecem proteção forte contra ataques de decodificação. Além disso, implementar a troca de chaves seguras, como o protocolo *Diffie-Hellman*, garante que apenas o cliente e o servidor envolvidos na comunicação tenham as chaves de criptografia para decifrar os dados.



Detecção

- Analisar *logs* e atividades: Analise regularmente os *logs* de eventos do sistema para detectar atividades suspeitas. Fique atento a tentativas de *login*, especialmente as que falharam, comportamentos incomuns, como acessos em horários anormais ou tentativas de acesso a recursos não-autorizados, ou alterações nas configurações.

- Implementar *firewalls* e sistemas de detecção de intrusões: Utilize *firewalls* para controlar e filtrar o tráfego de rede. Considere a implementação de sistemas de detecção de intrusões (IDS) ou prevenção de intrusões (IPS) para identificar e bloquear atividades maliciosas.
- Executar um monitoramento contínuo: o monitoramento de atividades suspeitas na rede e nos sistemas ajudará a identificar qualquer comportamento incomum ou tentativas adicionais de acesso não autorizado.

Tratamento e Resposta

- Segregar o dispositivo ou rede afetado: Assim que o ataque for identificado, isole imediatamente o sistema ou rede afetada, preferencialmente desconectando-o da *Internet* e isolando-o do restante da rede para evitar que o ataque se propague.

- Desativação do acesso remoto: Se possível, desative o acesso remoto comprometido, interrompendo o serviço RDP no sistema afetado. Isso ajudará a evitar que os invasores continuem explorando as vulnerabilidades.
- Coleta de evidências: É importante preservar qualquer evidência relacionada ao ataque. Registre detalhes sobre o incidente, incluindo *logs* de eventos, registros de atividade e quaisquer arquivos ou dados comprometidos.

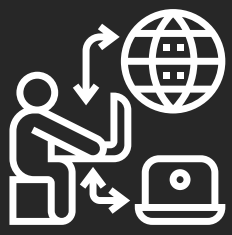
- Análise: Realize uma análise detalhada do sistema afetado para identificar a extensão do comprometimento e as possíveis vulnerabilidades exploradas. Remova qualquer *malware* ou *backdoors* encontrados e aplique correções de segurança para mitigar as vulnerabilidades exploradas.
- Alteração de senhas: Após o incidente, altere todas as senhas relacionadas ao acesso remoto, incluindo senhas de contas de usuário e senhas de administrador. Certifique-se de usar senhas fortes e exclusivas.

- Restauração a partir de *backups* confiáveis: Caso seja necessário, restaurar os sistemas afetados a partir de *backups* confiáveis. Certificar-se de que os *backups* não tenham sido comprometidos antes de realizar a restauração.

- Ações pós-incidente: Realize uma análise detalhada do incidente para entender como o ataque ocorreu e identificar possíveis melhorias nas políticas, práticas de segurança, configurações e treinamento de funcionários.

Exemplo de Ataque

Suponhamos que uma empresa chamada *Test Tec* esteja utilizando o acesso remoto através do protocolo RDP para permitir que seus funcionários trabalhem de forma remota. Um dos funcionários recebe um *e-mail* de *phishing* que parece ser de um fornecedor conhecido da empresa, solicitando que o funcionário clique em um *link* para visualizar uma orientação recente. Por não ter recebido a devida orientação de segurança, o usuário clica no *link*. Ao clicar no *link*, a conexão é redirecionada para um *site* malicioso que instala um *malware* no seu dispositivo.



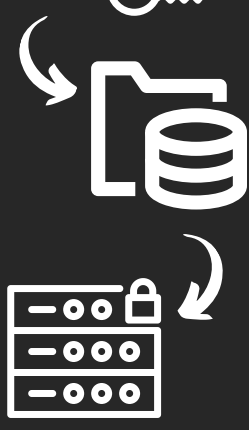
O invasor agora possui acesso não autorizado ao computador do funcionário, e verifica que ele tem permissões para se conectar remotamente ao sistema da *Test Tec*. O invasor utiliza ferramenta de força bruta, como o "*Hydra*" ou "*Ncrack*", para quebrar a senha do RDP. Como não há um limite de tentativas de *login* antes do bloqueio da conta, o invasor, após várias tentativas, é bem-sucedido e ganha acesso ao servidor RDP da empresa.

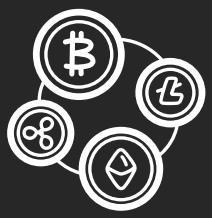
Com acesso ao sistema da *Test Tec*, o invasor utiliza uma ferramenta para verificar a existência de vulnerabilidades, como o Nmap. Ele verifica que a versão do servidor RDP não está atualizada com as últimas correções de segurança, como o *patch* para a vulnerabilidade CVE-2019-0708 (também conhecida como *BlueKeep*). Utilizando uma ferramenta como *Metasploit*, o invasor executa um *exploit* para escalar privilégios e ganhar acesso de administrador.

Com controle total sobre o servidor, o invasor inicia a movimentação lateral dentro da rede da *Test Tec*. Ele utiliza ferramentas, como o *BloodHound*, para fazer a enumeração da rede, identificando outros dispositivos vulneráveis e suas conexões.

Para exfiltrar dados confidenciais da *Test Tec*, o invasor utiliza uma ferramenta, como o *Mimikatz*, para obter as credenciais armazenadas em texto claro na memória dos sistemas comprometidos. Com essas credenciais, ele acessa bancos de dados e servidores de arquivos, copiando informações sensíveis para um servidor externo sob seu controle.

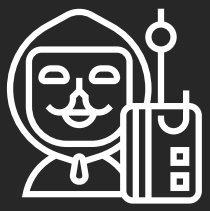
O invasor também verificou estar sendo utilizado o *Microsoft Server Message Block* v3 (MS-SMBv3), que é vulnerável ao CVE-2020-0796, que permite ao invasor executar código tanto no servidor SMB como no cliente SMB. O *Server Message Block* (SMB) é um protocolo de rede usado para compartilhamento de arquivos e outros recursos entre dispositivos em uma rede. O invasor se aproveita dessa vulnerabilidade utilizando um *exploit* de ataque cibernético como o *EternalBlue* para infectá-lo com um *ransomware*. Curiosamente, o *EternalBlue* foi desenvolvido pela Agência de Segurança Nacional (NSA) dos EUA como uma ferramenta para testar a proteção de redes.





O invasor conclui o ataque criptografando as redes descobertas na infraestrutura da *Test Tec*, utilizando um artefato *ransomware* fornecido por um grupo *Ransomware-as-a-Service* (RaaS), como *Conti* ou *Ryuk*. Os sistemas críticos ficam indisponíveis e a empresa é solicitada a pagar um resgate em criptomoedas, como *Bitcoin* ou *Monero*, para recuperar o acesso aos seus dados.

Este exemplo hipotético destaca como uma combinação de técnicas, ferramentas e vulnerabilidades podem ser exploradas em um ataque RDP. A seguir serão apresentadas algumas medidas que poderiam ter sido aplicadas para evitar cada uma das ações do atacante no exemplo da Test Tec.



- Prevenção do *phishing*: implementar treinamentos regulares de conscientização sobre segurança cibernética para os funcionários, ensinando-os a identificar *e-mails* de *phishing*. Além disso, a utilização de filtros de *spam* e sistemas anti-*phishing* pode ajudar a bloquear *e-mails* maliciosos antes que cheguem às caixas de entrada dos funcionários.

- Fortalecimento da autenticação: utilizar autenticação em dois fatores (2FA) para o acesso RDP, exigindo uma segunda forma de autenticação além das credenciais de login. Isso dificultaria o sucesso de ataques de força bruta.

- Atualização regular: manter o *software* RDP e outros sistemas atualizados com as últimas correções de segurança, incluindo patches para vulnerabilidades conhecidas, como o BlueKeep (CVE-2019-0708) mencionado no exemplo. Implementar um processo de gerenciamento de *patches* eficiente para garantir que as atualizações sejam aplicadas regularmente.

- Restrições de movimento lateral: implementar medidas de segurança, como a segmentação da rede e a aplicação de políticas de *firewall* adequadas, para limitar o movimento lateral dentro da rede. Isso ajuda a evitar que um invasor comprometa outros sistemas após a exploração bem-sucedida de um dispositivo.

- Boas práticas de segurança de dados: utilizar a criptografia nos dados sensíveis armazenados nos sistemas, garantindo que mesmo se um invasor obtiver acesso, os dados permanecerão ilegíveis. Além disso, realizar *backups* regulares dos dados e testar a restauração dos *backups* para garantir a disponibilidade e integridade dos dados em caso de ataque.

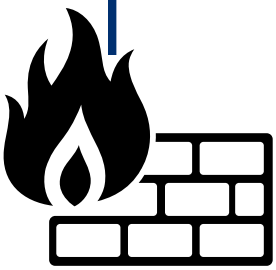
- Monitoramento de anomalias e atividades suspeitas: implementar soluções de monitoramento de segurança, como sistemas de detecção de intrusões (IDS) e sistemas de informações e eventos de segurança (SIEM), para identificar comportamentos anormais e atividades suspeitas dentro da rede. Isso permite a detecção precoce de tentativas de ataque e uma resposta imediata.

- Controle de acesso: utilizar controles de acesso granulares para restringir o acesso ao RDP apenas aos usuários autorizados. Isso pode ser feito através de políticas de grupo ou configurações de permissões adequadas.

- *Backup* e recuperação de desastres: manter um plano de *backup* e recuperação de desastres eficiente, com *backups* regulares dos dados críticos. Garantir que os *backups* estejam armazenados em locais seguros e testar periodicamente a restauração dos dados para verificar a sua integridade e disponibilidade.

Considerações finais

A segurança cibernética é um esforço contínuo de toda organização e deve ser motivada e suportada pelo alto escalão. Esta segurança envolve a implementação de várias camadas de proteção. As medidas mencionadas são apenas algumas das ações que poderiam ter sido aplicadas para evitar os diferentes estágios de um ataque, particularmente o descrito no exemplo. Uma abordagem abrangente de segurança cibernética deve incluir políticas, práticas e tecnologias adequadas para proteger os sistemas e dados contra ameaças em constante evolução.



Ao longo dessa OSIC, exploramos diversas estratégias de mitigação e resposta ante ataques contra o *Remote Desktop*. A implementação de políticas de segurança robustas, como o uso de autenticação de múltiplos fatores, senhas fortes e atualizações regulares do *software* RDP, é essencial para fortalecer a segurança do acesso remoto.

Além disso, a segmentação de rede, a utilização de *firewalls*, a configuração correta das permissões de acesso e a monitorização contínua dos *logs* de eventos são medidas-chave para detectar e prevenir ataques direcionados ao *Remote Desktop*.

Ao adotar medidas de proteção, as organizações estarão fortalecendo a segurança e reduzindo significativamente o risco de ataques cibernéticos bem-sucedidos. A proteção do acesso remoto é um elemento crítico para a segurança cibernética como um todo, e investir em medidas de segurança adequadas é essencial para manter a integridade, confidencialidade e disponibilidade dos sistemas e informações.

Complementarmente, a Secretaria de Segurança da Informação e Cibernética (SSIC) também recomenda aos usuários das diversas organizações, além das orientações apresentadas nesta OSIC, que:

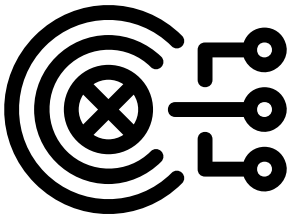
- atentem quanto as configurações inadequadas de autenticação, particularmente quanto a habilitação da *Network Level Authentication* (NLA);

- tenham atenção às boas práticas de *Secure-by-Design* (Segurança por projeto) quando a organização desenvolver sistemas que sejam expostos na *internet*;

- caso o RDP esteja configurado para ser acessível diretamente pela *Internet*, garanta proteções adequadas, para que ele não se torne um alvo atraente para ataques;

- eduque os usuários sobre as melhores práticas de segurança cibernética, como não compartilhar senhas e não clicar em *links* suspeitos; e

- informem imediatamente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) de sua instituição a ocorrência de um incidente cibernético.



Cabe destacar que a implementação de várias camadas de segurança é fundamental para uma proteção eficaz contra os ataques cibernéticos. Cada infraestrutura e sistemas podem ter requisitos específicos, portanto, é recomendável análise e configuração adequadas às necessidades da sua organização.

Outras Orientações de Segurança da Informação e Cibernética (OSICs) estão disponíveis em:

https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/osic

Propostas de temas, sugestões ou outras contribuições para serem abordadas em futuras OSICs podem ser encaminhadas ao e-mail: educa.si@presidencia.gov.br.

TLP:CLEAR