Resultados – Testes de Cibersegurança Compartilhados

Iniciativa do Grupo Consultivo de Cibersegurança

Novembro de 2019

INFORMAÇÕES GERAIS

No âmbito dos trabalhos do Grupo Consultivo de Cibersegurança da ANBIMA[1], entre 2018 e 2019, executou-se o programa piloto de *testes de penetração compartilhados* para instituições associadas.

A iniciativa, integrada ao Plano de Ação da Associação de 2019, foi formulada a partir dos resultados da pesquisa sobre cibersegurança no mercado local conduzida pelo Grupo, que busca mensurar o grau de maturidade e de aderência das instituições associadas às práticas recomendadas pelo Guia de Cibersegurança da ANBIMA. Com as edições anteriores da pesquisa, finalizadas em 2017 e 2018, percebeu-se que havia espaço para a condução de um projeto que fomentasse a cultura de testes de cibersegurança, particularmente no segmento de gestão de recursos.

Desse modo, a iniciativa dos testes de penetração compartilhados incluiu 15 gestoras associadas. Em cada empresa participante executou-se um teste baseado em Cenários de Ataques Avançados. O objetivo do teste era analisar a resiliência dos controles de segurança das instituições. O teste simulava uma ameaça motivada, dotada de recursos técnicos, que realizava ataques direcionados com o intuito de obter informações e dados sigilosos.

Os resultados dos testes foram reunidos em relatórios individualizados, entregues apenas para as empresas participantes. Como produto final da iniciativa, a ANBIMA recebeu um relatório que, sem permitir a identificação das participantes nos testes, trouxe um conjunto de recomendações gerais a serem seguidas para suprimir a superfície de ataque e possibilitar um aumento na segurança.

O presente documento tem como objetivo promover a divulgação dessas recomendações consolidadas, oriundas dos testes compartilhados. Ao todo, são 10 recomendações apresentadas abaixo, que abordam aspectos como bloqueio das extensões de arquivos por usuários até a definição de privilégios em uma rede. Essas recomendações pressupõem que o leitor possua alguma familiaridade com os conceitos de segurança da informação, desenvolvimento, tecnologia de redes, aplicações web e de administração de sistemas.

[1] Para mais informações sobre as iniciativas desenvolvidas pelo organismo, acesse: http://www.anbima.com.br/pt_br/representar/grupos-de-trabalho/ciberseguranca/ciberseguranca.htm

RECOMENDAÇÕES CONSOLIDADAS

1. Recebimento de artefatos maliciosos por meio de um navegador web

Recomendação

Deve-se bloquear o máximo de extensões possíveis, evitando desta forma que as mesmas possam ser recebidas e executadas pelos usuários. O ideal para tratar esse tipo de questão é modificar ou estabelecer uma política de acesso baseada em *whitelist*, onde as extensões vão sendo liberadas paulatinamente, após uma análise e avaliação básicas.

Mais informações

https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-asan-attack-vector/malware-delivery-in-phishing-campaigns/#gref

2. Recebimento de arquivo malicioso através de e-mail

Recomendação

Recomenda-se a revisão do filtro de conteúdo de e-mail, a fim de bloquear a lista de extensões exploradas, assim como qualquer extensão com potencial de execução de código direta ou indiretamente. Vale salientar que na medida em que os softwares são instalados nas estações, outras extensões passam a ser reconhecidas pelo sistema operacional e podem ser utilizadas para fins de execução de comando local redundando no comprometimento da estação.

Recomenda-se o bloqueio de arquivos protegidos por senha, pois os filtros de e-mail não podem decifrar e inspecionar arquivos com senha. Qualquer arquivo com uma senha deve ser bloqueado e uma análise do artefato deve ser executada para revelar a natureza de tal arquivo.

Adicionalmente, deve-se fazer um levantamento dos softwares disponíveis nas estações de trabalho e as extensões associadas aos mesmos, bem como bloquear o máximo de extensões possíveis, evitando que as mesmas possam ser recebidas e executadas pelos usuários. O ideal para sanar esse tipo de questão é modificar ou estabelecer uma política de acesso baseada em *whitelist*, onde as extensões vão sendo liberadas paulatinamente, após uma avaliação básica.

Por fim, de forma macro, a conscientização dos usuários por meio de treinamentos é uma abordagem efetiva para dirimir a superfície desse tipo de ataque. Para tal pode-se utilizar ferramentas de simulação de envio de *phishing* com intuito de propiciar o treinamento do usuário final contra esse tipo de ataque.

Mais informações

https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-asan-attack-vector/malware-delivery-in-phishing-campaigns/#gref

3. Estabelecimento de comando e controle através do protocolo HTTP

Recomendação

Recomenda-se a aplicação de regras de *firewall* mais restritivas, a fim de dificultar o estabelecimento de *connect backs* com servidores remotos. Deve-se bloquear o tráfego de saída para portas que não sejam fundamentais ao negócio. Adicionalmente, para as portas que precisam ser liberadas, recomenda-se o monitoramento de anomalias.

Vale salientar a importância da aplicação de uma política restritiva de navegação no proxy. Embora a utilização de *blacklists* de domínios surta algum efeito, a experiência mostra que atacantes eventualmente encontram brechas e abusam deste tipo de bloqueio para controlar estações de trabalho e vazar dados sensíveis.

Portanto, a aplicação de uma política de navegação baseada em *whitelist* é preferível, onde o mínimo de serviços é liberado para os usuários e, de acordo com a demanda de acessar sites fora da *whitelist*, deve-se avaliar a necessidade e o risco de se permitir tal acesso.

Mais informações

https://docs.microsoft.com/pt-br/security-updates/SecurityBulletins/2014/ms14-025#classifica%C3%A7%C3%A3o-de-gravidade-e-identificadores-devulnerabilidade--

4. Vazamento de informações sensíveis através de emails e formulários web

Recomendação

Recomenda-se a verificação das regras de DLP (*Data Loss Prevention)*, a fim de mitigar o vazamento de informações sensíveis pelos mais diversos vetores.

Mais informações

https://www.symantec.com/pt/br/products/dlp

5. Possibilidade de vazamento de dados através do Tor e SSH

Recomendação

Recomenda-se a aplicação de regras de *firewall* mais restritivas a fim de impedir a navegação na rede Tor. Os principais fornecedores de *firewalls* possuem recursos para a identificação e o bloqueio do tráfego dessa rede. Bloqueios também podem ser realizados através scripts que realizam filtros, através de consultas em bases públicas de "nós" da rede Tor.

Recomenda-se o bloqueio de conexões SSH caso seu uso não se faça necessário, e a realização de uma análise de tráfego a fim de verificar conexões SSH em portas distintas.

É importante ainda identificar quais aplicações são autorizadas a serem executadas no sistema, baseando-se em regras de *whitelisting* para garantir o uso apenas de softwares autorizados. Para garantir que a *whitelist* seja implementada de forma correta, testes deverão ocorrer em busca de falhas de configuração através das permissões dadas aos arquivos instalados no sistema.

Por fim, cumpre lembrar que a *whitelist* não deve substituir softwares como antivírus e outros softwares de segurança. Além disso, usar múltiplas soluções agregadas de segurança pode contribuir para uma defesa mais efetiva do sistema.

Mais informações

https://www.symantec.com/pt/br/products/dlp

6. Possibilidade de execução do PowerShell

Recomendação

É recomendável que a execução do PowerShell seja restrita apenas aos usuários que executem tarefas administrativas nas estações de trabalho. O bloqueio do PowerShell pode ser realizado através da aplicação de regras do AppLocker, restringindo a quais grupos ou usuários as regras serão aplicadas.

É de extrema importância que sejam realizados testes em ambiente de homologação para avaliar os impactos no funcionamento do sistema e aplicações instaladas no sistema operacional. Além dos testes, recomenda-se também que a aplicação das regras de bloqueio no ambiente de produção seja primeiramente realizada no modo de auditoria, a fim de identificar possíveis bloqueios indesejados.

O processo de bloqueio do PowerShell através do AppLocker possui algumas etapas, sendo estas resumidas da seguinte forma:

1) Criação de uma GPO específica para este fim;
2) Configuração das regras padrão para a execução de aplicativos;
3) Configuração das exceções que irão, de fato, realizar o bloqueio do PowerShell;

4) Configuração do *enforcement* das regras, sendo primeiramente recomendado o modo de auditoria e só após a análise dos logs e confirmação do correto funcionamento, a troca para o modo de *enforcement* de regras;

5) Realização de testes do bloqueio e monitoramento.

Para cada passo descrito acima existem detalhes a serem observados, tais como: a seleção dos grupos e usuários, seleção da ação da regra, configuração das exceções, entre outros. Por se tratar de um procedimento detalhado e minucioso, recomenda-se fortemente a leitura dos materiais disponíveis pelo fabricante para a correta implementação da solução.

Mais informações

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-policies-deployment-guide

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/working-with-applocker-rules

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/configure-exceptions-for-an-applocker-rule

7. Possibilidade de acessar servidores SMB na Internet

Recomendação

Recomenda-se bloquear todo o tráfego de saída referente ao protocolo SMB no *firewall*.

Mais informações

https://technet.microsoft.com/pt-br/library/hh831795.aspx

8. Possibilidade de burlar restrições de rede através de túneis DNS e ICMP

Recomendação

Recomenda-se bloquear no firewall todo o tráfego de saída referente a protocolos que não sejam imprescindíveis ao negócio, como por exemplo ICMP e SSH. Tais protocolos podem ser abusados para controlar remotamente as estações de trabalho, assim como vazar dados sensíveis.

Recomenda-se também o monitoramento do protocolo DNS, a fim de identificar tráfegos anômalos.

Mais informações

https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

https://hackersterminal.com/dns-tunneling/

9. Persistência na estação de trabalho comprometida

Recomendação

Recomenda-se que usuários menos privilegiados não tenham a permissão de agendar tarefas em suas estações. Um recurso que pode auxiliar esta ação é a criação de diretivas de grupo (GPOs). Caso a liberação seja necessária, recomenda-se estabelecer o monitoramento dos agendamentos criados pelos usuários.

Recomenda-se restringir a possibilidade de alteração de chaves de registro exclusivamente a usuários privilegiados.

Recomenda-se ainda remover as permissões dos usuários sem privilégios na pasta Startup de estações.

Mais informações

https://resources.infosecinstitute.com/common-malware-persistence-mechanisms/#gref

10. Escalação de privilégios

Recomendação

Recomenda-se a atualização dos servidores de domínio a fim de mitigar a vulnerabilidade catalogada de acordo com o CVE-2014-1812.

A atualização modifica o **Editor de Diretivas de Grupo**, removendo a capacidade de configurar e distribuir senhas usando as seguintes extensões de preferências de Diretiva de Grupo:

- Mapeamento de unidades;
- Configurar usuários e grupos locais;
- Configurar tarefas programadas;
- Configurar serviços;
- Configurar fontes de dados.

É importante observar que a atualização não remove quaisquer GPOs existentes que foram configurados antes da aplicação desta atualização de segurança. Os clientes com GPOs existentes que foram configurados usando as preferências identificadas da Diretiva de Grupo devem remover esse risco do seu ambiente de domínio.

Mais informações

https://docs.microsoft.com/pt-br/security-updates/SecurityBulletins/2014/ms14-025#classifica%C3%A7%C3%A3o-de-gravidade-e-identificadores-de-vulnerabilidade-