Por Alexandre Sammogini

Desde os primórdios, a relação de contar – ou computar – já intrigava a humanidade. Fazendo valer este argumento, podemos pensar que a criação de computadores teve início na idade antiga, com a criação do “ábaco”, no século V a.C., como o primeiro instrumento mecânico de computação.

Antes do advento de computadores dotados com algum tipo de telecomunicação, a conexão entre máquinas calculadoras e computadores antigos era realizada por usuários humanos através do carregamento de instruções entre eles. De lá pra cá, grandes avanços vêm sendo conquistados com destaque para a evolução gradual das redes de sistemas computacionais nas décadas de 1950 e 1960, 1970, 1980, 1990 e anos 2000.

Os avanços de revoluções digitais ocorridos em todo mundo nas últimas décadas, e principalmente neste momento de pandemia, sem dúvida trouxeram muitas melhorias para a vida pessoal e corporativa, colocando o universo em uma perspectiva de uma grande rede de informações. No entanto, este universo traz consigo também um ar de complexidade em relação a exposição a risco e segurança da informação, o que exige uma eficaz gestão dessas redes.

O gerenciamento de rede ocupa uma posição estratégica nos negócios. Tal fato pode ser verificado no filme: O jogo da imitação (2014), cuja sinopse nos traz:

“Nada mais nada menos que um filme sobre Alan Turing. Conhecido como o pai da computação e no desenvolvimento de algoritmos. Neste filme, um drama sobre uma história real passada durante a Segunda Guerra Mundial, Turing trabalha para inteligência britânica especializada em quebra de códigos.

No filme vemos Turing trabalhando para conseguir desencriptar mensagens alemãs. Ao conseguir quebrar os códigos criptografados dos alemães, ele deu uma grande vantagem aos aliados, o que resultou no principal fator para o fim da Segunda Guerra Mundial.”

Uma boa estrutura de tecnologia da informação é essencial para que seus dados não estejam apenas ordenados, mas também seguros. Sem gestão de rede, temer pela segurança dos seus dados é uma realidade justificada, pois são altos os riscos de sofrer ataques ou roubos de informações, conforme sinopse do filme apresentada.

A seguir, é apresentado resumo com sugestões de práticas que devem ser considerados na busca de segurança da informação, dentro das organizações, em relação à gestão de segurança em redes, conforme Checklist-ISO27701 e Cys Controls – Frameworks.

Três Fontes de Data / Hora Sincronizadas	Utilizar, pelo menos, três fontes de tempo sincronizadas a partir das quais todos os servidores e dispositivos de rede recuperam informações de tempo regularmente, para que os registros de data e hora nos logs sejam consistentes.
Activate Audit Logging	Verificar se o armazenamento de logs locais foi ativado em todos os sistemas e dispositivos de rede.
Enable Detailed Logging	Habilitar logs de sistema para incluir informações detalhadas, como origem do evento, data, usuário, registro de data e hora, endereços de origem, endereços de destino e outros elementos úteis.
Ensure Adequate Storage for Logs	Validar que todos os sistemas que armazenam logs possuem espaço de

	armazenamento adequado para os logs gerados.
Central Log Management	Validar que os logs apropriados estão sendo agregados a um sistema central de gerenciamento de logs para análise e revisão.
Deploy SIEM or Log Analytic Tools	Implementar um sistema de SIEM (Gerenciamento de informações e eventos de segurança) ou uma ferramenta analítica que realize análise e correlação de logs.
Regularly Review Logs	Revisar regularmente os logs para identificação de anomalias ou eventos anormais.
Regularly Tune SIEM	Realizar regularmente o ajuste do sistema de SIEM para melhor identificação e filtragem de eventos que gerem acionamento a fim de que haja uma maior precisão na identificação de eventos.
Filtros de URL Estruturados na Rede	Impor filtros de URL na rede que limitem a capacidade de um sistema em se conectar a sites não aprovados pela organização. Essa filtragem deve ser aplicada a cada um dos sistemas da organização, estejam eles fisicamente nas instalações da organização ou não.
Serviços de Categorização de URL	Providenciar assinatura de serviços de categorização de URL para garantir que os browsers estejam atualizados com as definições de categorização de sites mais recentes disponíveis. Sites não categorizados devem ser bloqueados por padrão.
Logs de Todas as URL	Registrar todas as solicitações de URL de cada um dos sistemas da organização, seja localmente ou em dispositivos móveis, a fim de identificar atividades potencialmente maliciosas e ajudar o time de segurança da informação a identificar sistemas potencialmente comprometidos.
Serviços de Filtragem de DNS	Utilizar os serviços de filtragem de DNS (Sistema de Nomes de Domínio) para ajudar a bloquear o acesso a domínios maliciosos conhecidos.
DMARC	Implementar diretiva de verificação automática de mensagens, relatórios e conformidade (DMARC) baseadas em domínio, iniciando pela implementação dos padrões Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM) para diminuição de chance de recebimento de e-mails falsificados ou modificados oriundos de domínios válidos.
Arquivos Desnecessários	Bloquear todos os anexos de e-mail que entram no gateway de e-mail da organização filtrando os tipos de arquivo desnecessários para os negócios da organização.
Sandboxes Para Anexos de E-mails	Utilizar Sandboxes para analisar e bloquear anexos de e-mail nas caixas de entrada que possuam comportamento malicioso.
Logs Registrando Consultas ao DNS	Habilitar os logs de consultas do DNS (Sistema de Nomes de Domínio) para detectar pesquisas de nomes de host para domínios maliciosos conhecidos.
Configurações de Segurança Padrão Para Dispositivos de Rede	Manter padrões de configuração de segurança documentados para todos os dispositivos de rede

	autorizados.
Regras de Configuração de Tráfego	Documentar todas as regras de configuração que permitem que o tráfego flua através de dispositivos de rede em um sistema de gerenciamento de configurações abrangendo: uma justificativa do negócio específica para cada regra aplicada, o nome de um indivíduo específico responsável para cada regra, um descritivo da necessidade comercial que demandou a criação da regra e a duração esperada da configuração aplicada.
Ferramentas Automatizadas Para Verificação das Configurações Padrão de Dispositivos	Realizar um comparativo de toda a configuração dos dispositivos de rede com as configurações de segurança aprovadas definidas para cada dispositivo de rede em uso, reportando quaisquer desvios encontrados.
Versão Estável Mais Recente de Qualquer Atualização Relacionada à Segurança em Todos os Dispositivos de Rede	Manter todos os dispositivos de rede sempre atualizados com os patches de segurança mais estáveis e recentes.
Dispositivos de Rede Utilizando Autenticação Multifator e Sessões Criptografadas	Gerenciar todos os dispositivos de rede utilizando padrão de autenticação MFA e sessões encriptadas.
Máquinas Dedicadas Para Todas as Tarefas Administrativas de Rede	Garantir que os arquitetos e analistas de redes utilizem uma máquina dedicada para todas as tarefas administrativas ou tarefas que exijam acesso elevado. Esta máquina deve ser segmentada da rede principal da organização e não deve ter acesso à Internet. Esta máquina não deve ser usada para ler e-mails, compor documentos ou navegar na Internet.
Infraestrutura de Rede por Meio de uma Rede Dedicada	Gerenciar a infraestrutura de rede através de conexões de rede separadas do uso comercial desta rede, se apoiando em VLANs separadas ou, preferencialmente, em conectividade física totalmente diferente para sessões de gerenciamento de dispositivos de rede.
Inventário dos Limites de Rede	Manter um inventário atualizado de todos os limites de rede da organização.
Conexões não Autorizadas em Limites de Rede Confiáveis	Executar verificações regulares de fora de cada limite de rede confiável para detectar qualquer possível vetor de conexão não autorizada acessível por fora do limite.
Comunicações Oriundas de Endereços IP Maliciosos Conhecidos	Negar comunicações oriundas de endereços IP maliciosos conhecidos ou não utilizados da internet e limitar o acesso apenas a intervalos de endereços IP confiáveis e necessários em cada um dos limites de rede da organização.
Negar comunicações em Portas Não Autorizadas	Realizar o bloqueio de comunicações com endereços IP da Internet que sejam conhecidamente maliciosos ou não utilizados e realizar a limitação do acesso apenas a intervalos de endereços IP confiáveis e necessários em cada um dos limites de rede da organização.
Sistemas de Monitoramento Para Registrar Pacotes de Rede	Configurar os sistemas de monitoramento para registrar pacotes de rede que passam por cada um dos limites de rede da organização.
Sistema de Sensores IDS na Rede	Implementar sensores IDS (Intrusion Detection

	Systems) na rede para procurar mecanismos de ataque incomuns e detectar comprometimentos desses sistemas em cada um dos limites de rede da organização.
Sistemas de Prevenção a Intrusões na Rede	Implementar sistemas de prevenção de intrusões (IPS) na rede para bloquear o tráfego malicioso da rede em cada um dos limites de rede da organização.
Coleção NetFlow em dispositivos de Borda de Rede	Habilitar a coleta de dados do NetFlow e de logs em todos os dispositivos de borda de rede.
Servidor Proxy de Filtragem de Camada de Aplicativo	Verificar se todo o tráfego de rede de ou para a Internet passa por um proxy da camada de aplicativos autenticado, configurado para filtrar conexões não autorizadas.
Tráfego de Rede no Proxy	Descriptografar todo o tráfego de rede criptografado no proxy de borda antes de analisar o conteúdo. No entanto, a organização pode usar uma lista de sites permitidos que podem ser acessados por meio do proxy sem descriptografia do tráfego.
Segmentação de Rede com Baseada na Classificação de Informações	Segmentar os dados trafegados na rede através de data tagging (etiquetação de dados) ou níveis de classificação da informação armazenada nos servidores, varredura de todas as informações sensíveis em Vlans apartadas da rede principal.
Filtragem de Firewall Entre VLANs	Habilitar a filtragem de firewall entre VLANs para garantir que apenas sistemas autorizados possam se comunicar com outros sistemas críticos para execução suas funcionalidades específicas.
Comunicação Entre Estações de Trabalho	Desativar toda a comunicação de estação de trabalho para estação de trabalho por meio de tecnologias como VLANs privadas ou micro segmentação para limitar a capacidade de um invasor realizar movimentações laterais e comprometer os sistemas vizinhos.
Inventário de Pontos de Acesso Wireless Autorizados	Manter um inventário de pontos de acesso sem fio autorizados conectados à rede cabeada.
Pontos de Acesso Sem Fio Conectados à Rede Com Fio	Configurar ferramentas de verificação de vulnerabilidade de rede para detectar e alertar sobre pontos de acesso sem fio não autorizados conectados à rede cabeada.
Sistema de Detecção de Intrusão em Redes Sem Fio	Utilizar um sistema de detecção de intrusão sem fio (WIDS) para detectar e alertar sobre pontos de acesso sem fio não autorizados conectados à rede.
Padrão AES (Advanced Encryption Standard) Para Criptografar Dados Sem Fio	Elevar a criptografia de dados sem fio em trânsito para o Padrão Avançado de Criptografia (AES).
Protocolos de Autenticação Sem Fio	Verificar se as redes sem fio utilizam protocolos de autenticação como EAP/TLS (Extensible Authentication Protocol – Transport Layer Security), que requeiram autenticação com a utilização de vários fatores (MFA).
Rede Sem Fio Separada Para Dispositivos Pessoais e Não Confiáveis	Realizar a criação de uma rede sem fio separada para dispositivos pessoais ou não confiáveis. O acesso corporativo desta rede deve ser tratado

	como não confiável, filtrado e auditado de acordo.
Firewalls de Aplicativos da Web (WAF)	Proteger os aplicativos da Web implementando firewalls de aplicativos da Web (WAFs) que inspecionem todo o tráfego que flui para as aplicações web em busca de ataques comuns a este tipo de aplicação. Para aplicativos que não são baseados na Web, firewalls de aplicativos específicos devem ser implementados se essas ferramentas estiverem disponíveis para o tipo de aplicativo especificado. Se o tráfego estiver criptografado, o dispositivo deve ficar atrás da criptografia ou ser capaz de descriptografar o tráfego antes da análise. Se nenhuma opção for apropriada, um firewall de aplicativo da web baseado em host deve ser implantado.
Exercícios de Red Team Periódicos	Realizar exercícios periódicos da equipe de red team para testar o grau de prontidão da organização em identificar, interromper ataques de forma rápida e eficaz.

Bom Pessoal! O ano de 2021, ao contrário do que se imaginava, está chegando ao fim. Nossa Comissão fará um pequeno recesso para as comemorações de fim de ano. Desejamos a todos um Feliz Natal e um 2022 mais seguro para todos. Retornaremos, no início do próximo ano, como mais uma edição. Não percam o “Saiba como tornar seus processos de T.I. robustos e capazes de prevenir ataques cibernéticos – Parte V”

*Comissão Técnica de Governança e Riscos da Regional Leste.

Fonte: Abrapp em Foco, em 29.11.2021.