Artigo: Saiba como tornar seus processos de T.I. robustos e capazes de prevenir ataques cibernéticos. – Pela CT Leste de Governança e Riscos

---

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 Tempo Sincronizadas	Utilizar pelo menos três fontes de tempo sincronizadas a partir das quais todos os servido
Activate Audit Logging	Verificar se o armazenamento de logs locais foi ativado em todos os sistemas e dispositivos c
Enable Detailed Logging	Habilitar o logging do sistema para incluir informações detalhadas, como origem do evento, data, u
Ensure Adequate Storage for Logs	Verificar se todos os sistemas que armazenam logs possuem espaço de armazenamento ade
Central Log Management	Verificar se os logs apropriados estão sendo agregados a um sistema central de gerenciame
Deploy SIEM or Log Analytic Tool	Implementar o uso de SIEM (Gerenciamento de informações e eventos de segurança)
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 e
Filtros de URL para Tráfego de Rede	Implementar filtros de URL que limitem a capacidade de um sistema em se conectar a sites
Serviços de Categorização de URL	Habilitar serviços de categorização de URL para garantir que os browsers
Logs de Pesquisa de URL	Registrar todas as solicitações de URL de cada um dos sistemas da organização, seja localm
Serviços de Filtragem de DNS	Utilizar serviços de filtragem de DNS (Sistema de Nomes de Domínio) para ajudar a bloqu
DMARC	Implementar diretiva de verificação automática de mensagens, relatórios e conformidade (DM
Arquivos de Anexos de E-mail	Bloquear tipos de arquivos anexos de e-mail que entram no gateway de e-mail da organização filtranc
Sandboxes para Anexos de E-mail	Utilizar Sandboxes para analisar e bloquear anexos de e-mail nas caixas de entrada que pos
Logs Registrados de Consultas DNS	Habilitar os logs de consultas do DNS (Sistema de Nomes de Domínio) para detectar pesquis
Configurações de Segurança	Manter as configurações de segurança padrão de dispositivos de rede documentados para todos os dispositivos de r
Regras de Configuração de Tráfego	Configurar regras de configuração que permitem que o tráfego flua através de disp
Ferramentas Automatizadas de Verificação de Configuração	Realizar automaticamente verificações de configuração de dispositivos de rede com as configuraçõ
Versão Estável Mais Recente	Verificar se todos os dispositivos de rede estão executando a versão estável mais recente do software
Dispositivos de Rede Autenticados	Garantir que todos os dispositivos de rede exijam autenticação multifator, como MFA e sessões en
Máquinas Dedicadas para Tarefas Administrativas	Usar uma máquina dedicada para todas as tarefas administrativas de rede
Infraestrutura de Rede Dedicada	Manter a rede de infraestrutura de rede separada do uso comercial
Inventário de Limites de Rede	Manter um inventário atualizado de todos os limites de rede da organização.

Conexõ [illegible] de rede confiável para detectar qualque
Comuni [illegible] conhecidos ou não utilizados da i
Negar c [illegible] endereços IP da Internet que sejam conhecidame
Sistemas de [illegible] pacotes de rede que passam por cad
Sistema [illegible] (Intrusion Detection Systems) na rede para procurar mecanismos
Sistemas [illegible] de intrusões (IPS) na rede para bloquear o tráfego malic
Coleção [illegible] logs em todos os dispositivos de borda de rede.
Servidor [illegible] a Internet passa por um proxy da camada de a
Tráfego [illegible] o tráfego de rede criptografado no proxy de borda antes de analisar o co
Segmen [illegible] (etiquetação de dados) ou n
Filtragem [illegible] entre VLANs para garantir que apenas sistemas autorizados p
Comuni [illegible] estação de trabalho para estação de trabalho por meio de t
Inventár [illegible] sem fio autorizados conectados à rede cabeada.
Pontos d [illegible] bilidade de rede para detectar e alertar sobr
Sistema [illegible] sem fio (WIDS) para detectar e alertar sobre pon
Padrão [illegible] ado de Criptografia (A
Protoco [illegible] utilizam protocolos de autenticação como EAP/TLS (Extensible
Rede Se [illegible] tivos pessoais ou não confiávei
Firewall [illegible] implementando firewalls de aplicativos da Web (WAFs) que i
Exercíc [illegible] da equipe de red team para testar o grau de prontidão da orga

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.