SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
INSTITUTO NACIONAL DE EDUCAÇÃO DE SURDOS-INES

Nota Informativa

Todas as implementações realizadas no ambiente de Tecnologia deste Instituto são baseadas nas melhores práticas do mercado mundial, seguindo normas e propostas para implementar um Sistema de Gerenciamento de Segurança da Informação (SGSI) com o objetivo de chegar o mais próximo possível sem perder agilidade do cumprimento da norma ISO/IEC 27001, que define os requisitos para que os mecanismos de controle consigam garantir a confidencialidade, integridade e disponibilidade da informação.

A implementação destas soluções tem o objetivo de minimizar os riscos, proteger os dados sensíveis do Instituto e usuários internos / externos e manter a disponibilidade do ambiente de Tecnologia da Informação. Foram implementadas políticas e regras de segurança baseadas em tecnologias / plataformas de Next Generation Firewall, que trazem uma visibilidade dos acessos internos e externos, assim como controle de acesso à sites maliciosos, filtro de conteúdo, etc.

Com o intuito de proteger o investimento realizado e atuar dentro das melhores práticas indicadas pelas normas do Sistema de Gerenciamento de Segurança da Informação (SGSI), serão ativadas todas e quaisquer políticas que possam trazer mais proteção aos dados e ambientes, que tiverem disponíveis na plataforma e suas licenças contratadas.

Através de relatórios emitidos pela fabricante da Plataforma de Next Generation Firewall, em produção neste Instituto, foram levantadas informações importantes que nortearam a equipe de segurança a implementar políticas para bloquear ações indevidas de usuários, controlar o acesso à URLS através de categorização e filtros de conteúdo, assim como manter e criar novas regras no firewall para proteção contra tentativas de invasão, proteção avançada contra phishing e malwares conhecidos e desconhecidos, etc.

Alguns resultados deste relatório, durante o levantamento por um período de 30 dias:

- Foram verificados 52 aplicativos de alto risco, incluindo aqueles que podem introduzir ou ocultar atividades maliciosas, transferir arquivos fora da rede ou estabelecer comunicação não autorizada;
- Foram encontradas 3.828.433 ameaças totais na rede, incluindo exploits de vulnerabilidade, malware conhecidos e desconhecidos, bem como atividades de comando e controle (Botnets);
- 260 eventos de malware conhecidos e 314 eventos de malware desconhecidos foram observados no Instituto;
- Foi identificado uma quantidade grande de transferência de arquivos via WhatsApp WEB;
- Acessos às mídias sociais e aplicativos de vídeos de forma descontrolada, que também podem trazer riscos.
- O filtro avançado de acesso às URLs identificou 320 endereços IP maliciosos por trás desses URLs/domínios maliciosos. Esses endereços IP podem ser usados como infraestrutura C2 para exfiltrar dados, fornecer malware ou enviar comandos remotos para um sistema em sua rede.
- O filtro avançado de acesso às URLs identificou 1.241 solicitações maliciosas. Essas solicitações maliciosas incluem ransomware, malware, phishing, comando e controle e grayware.

De forma conclusiva, podemos dizer que esta solução de segurança, com a visibilidade e tratativa que está sendo realizada, está trazendo a segurança necessária aos dados e usuários deste Instituto.

Foi verificado acesso à algumas aplicações que trazem vulnerabilidades e foi observado que uma aplicação está entregando malware para o Instituto, se não houvesse um controle e visibilidade destas vulnerabilidades, o resultado poderia ser uma catástrofe na nossa rede, como temos visto em outras organizações, que divulgam de forma pública, ocorrências de sequestro de dados e perdas em suas aplicações críticas.

Outros resultados de análises feitas na plataforma, dados de um período de 30 dias:

- Mais de 60.000 (sessenta mil) logs de tentativas de acessos bloqueados de aplicações como TeamViewer, indicado como APP NOCIVO ao Instituto.
- Mais de 20.800 (vinte mil e oitocentos) logs de acessos WEB na categoria de GAMES, o que não é uma ação indicada para um ambiente corportativo;
- Com esses acessos WEB não indicados, houve um resultado de retorno de aproximadamente 1.600 (mil e seiscentos) logs bloqueados no firewall com possíveis malwares e quase 300 (trezentos) logs bloqueados com possível categoria de phishing (roubo de credenciais).

As recomendações, para garantir a continuidade destas tratativas internas e evitar estes incidentes de segurança, assim como possíveis problemas para a nossa Instituição são as seguintes:

- Implementação, manutenção e controle de políticas de habilitação de aplicativos seguros, permitindo apenas aplicativos necessários para os negócios fins do Instituto e aplicando controle granular a todos os outros;
- Abordagem dos aplicativos de alto risco com o potencial para abuso, como acesso remoto, compartilhamento de arquivos ou túneis criptografados;
- Abordagem da comunicação de comando e controle examinando a rede ou a fonte do host. As soluções de detecção e resposta ou registro podem fornecer uma indicação do que ocorreu;
- Manutenção do controle e proibição de acessos à URLs não indicadas, com a categorização nomeada como GAMES, MALICIOSOS, ADULTOS, etc.

Assim, os equipamentos e recursos tecnológicas devem ser utilizados para as atividades institucionais. Portanto, não é recomendável qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação de hardware e/ou software e acesso a sites que não tenham relação com as atividades administrativas ou pedagógicas, sem o

conhecimento prévio e o acompanhamento dos Técnicos de TI do Instituto. As áreas que necessitarem de tais demandas deverão solicitá-las por meio de abertura de chamada técnico via *Helpdesk.*

Por fim, pedimos desculpas pela ocorrência de algum transtorno decorrente das medidas adotadas e garantimos que todos os acessos necessários para as atividades profissionais serão atendidos com a máxima celeridade possível.

Os relatórios emitidos da plataforma de segurança, assim como todos os indícios dos logs exportados pelo firewall estão de posse da Divisão de Informática e estarão livres à leitura e avaliação dos servidores deste Instituto.

Rio de Janeiro, 15 de maio de 2023.

Sólange Maria da Rocha

Diretora Geral do Instituto Nacional de Educação de Surdos - INES