Documento de normas para incidente de vazamento de fotos pessoais dos clientes da Empresa S.A. para a internet. ATUALIZADO

Preparação:
>Diretriz:
Tendo identificado o incidente, é de extrema necessidade da Empresa S.A. o informe a todos da equipe envolvida na manutenção do computador do cliente. Buscando assim a organização entre eles e a preparação para a aplicação das diretrizes de resposta a incidente, tendo essas sido pré estabelecidas nas políticas anteriormente vistas da Empresa S.A. Os colaboradores após o informe devem manter a calma e começar o quanto antes a analise para contenção dos danos, pois o vazamento de dados pessoais dos clientes ameaça quebrar a imagem de mercado da Empresa S.A. que baseasse na confiança prestador -> cliente. Os colaboradores envolvidos devem estar plenamente capacitados para atender gentilmente o cliente quando este retornar assustado questionando sobre suas informações vazadas.
>Exemplo:
Jorge Rodrigues, um dos Técnicos de Suporte responsável pela manutenção dos notebook, percebeu durante suas atividades que o computador do cliente N2031 está contaminado com um vírus da classe Trojan, pois a cada hora que se passava com Jorge, os dados aos poucos sumiam do dispositivo. O notebook do cliente já veio contaminado, entretanto Jorge demorou para nota-lo. Assim que percebeu a ameaça, Jorge isolou o computador da rede da Empresa S.A. e buscou informar seu superior de departamento a Analista de Suporte Fernanda Dias, que ao receber essa informação, alertou o time de suporte sobre o Trojan identificado e o cliente N2031; repassando para o gestor de departamento Arthur Morais.

Detecção e Análise:
>Diretriz:
Com a equipe devidamente alertada e preparada, deve-se iniciar a analise em busca de quais informações do cliente foram vazadas e qual o peso delas para ele. Tendo essas informações, a equipe deve direcionar os esforços para a identificação do COMO, POR ONDE e PORQUE esses dados foram vazados, é de suma importância nesta etapa identificar o POR ONDE pois o vazamento pode significar uma quebra na segurança da rede de toda a Empresa S.A. pondo em risco não somente os dados de vários clientes com a integridade sistêmica da empresa. A identificação do POR ONDE juntamente de COMO auxiliaram diretamente na contenção de danos, sendo informações cruciais, já o PORQUE abre (ou não) o leque para o acionamento de autoridades afim de investigação criminal.
>Exemplo:
Arthur Morais decretou estado de emergência na sala da manutenção de Notebook, onde esse, ordenou o isolamento da rede da sala para com o resto da empresa. Após o isolamento, Arthur coordenou uma reunião com todo o time de suporte para levantar informações e preparar as atividades. Tendo feito isso, foi ordenado que o time de Técnicos de Suporte ficaram responsáveis por: garantir a integridades dos dados dos outros dispositivos em manutenção na sala, buscando o POR ONDE; os Analistas de Suporte N1 e N2 estariam responsáveis por: monitorar e analisar toda a rota do computador do cliente N2031 e noticias sobre (Redes sociais, e-mails de contato, telefones), buscando o PORQUE; o Técnico de Segurança da Informação Matheus Martins ficara responsável por: Analisar, categorizar e assegurar a não infecção de outros dispositivos nas proximidades ou do próprio cliente como através de serviços de Nuvem integrados, buscando o COMO.

Contingência:
>Diretriz:
Tendo as devidas informações de origem a Empresa S.A. deve-se isolar a maquina, por onde foi identificado o ataque, da rede; podendo ser utilizado de qualquer métodos decididos pelos colaboradores que não firam o patrimônio. Neste momento a equipe responsável deve organizar-se em três principais grupos, 1. Responsável pelo controle da maquina isolada, 2. Responsável por monitorar a infraestrutura da Empresa S.A. afim de garantir que não aja infecção em/para outros dispositivos da rede, 3. Responsável por capturar o trajeto dos dados vazados dentro das redes, afim de identificar possíveis autores. Tendo como principal objetivo identificar QUEM e o impacto que os dados causados podem causar.
>Exemplo:
Após o inicio das análises e contingências, Arthur Morais acionara além do time já exposto, a responsável Técnico de Infraestrutura Giovana Castro que informada do incidente tomara as devidas precauções dentro da infraestrutura (já isolada) da Empresa S.A. Levantando bloqueios de tráfico de dados na rede interna que monitorem cada informação trafegada a fim de encontrar padrões comprometedores. Arthur, junto da equipe de Analistas de Suporte buscara identificar possíveis responsáveis pelo incidente (QUEM), afim de informar a Direção da Empresa S.A. Observo que neste momento caso o incidente tenha passado de 24h o Arthur obrigatoriamente alertara a Direção sobre o estado de emergência da sala.

Erradicação:
>Diretriz:
Identificado o COMO, POR ONDE, PORQUE, QUEM e IMPACTO; a equipe envolvida no incidente deve acionar as autoridades caso necessário, e utilizar de todo o escopo técnico na elaboração de planos corretivos respectivos a cada área de atuação, tendo o corpo técnico TI o foco na infraestrutura, o corpo técnico RH o foco na elaboração de ações judicias e escopos de relações publicas da Empresa S.A. com o cliente e as autoridades, e o corpo técnico administrativo o foco no tocar das atividades da empresa apesar do incidente em ocorrência. Os colaboradores devem buscar a documentação de validação das medidas tomadas, unindo ao reforço na segurança de processos e interfaces dos usuários da Empresa S.A. afim de evitar-se semelhante ocorrido dentro de um curto período.
>Exemplo:
Tendo o COMO, POR ONDE, PORQUE, QUEM e o IMPACTO causado pelas informações capturadas, Arthur Morais, Giovana Castro e Matheus Martins se reuniram para compartilhar cada informação coletada sobre o incidente, buscando sempre a solução mais prática, que neste caso corresponde a: informar o cliente pessoalmente sobre o incidente (assegurando que ele possui as informações de login de todas as contas registradas em seu notebook, orientando-o a troca de senhas das contas), isolar e copiar de forma segura os dados da máquina do cliente para um Backup Local, Formatar o notebook e reconfigurar o setup para o mais semelhante ao original antes da formatação, varrer a infraestrutura da Empresa S.A., reiniciar o ramal responsável pela sala de manutenção de Notebook, alterar senhas das contas internas e locais presentes no ramal.

Restauração:
>Diretriz:
Após a contenção e entendimento do incidente de segurança ocorrido, a Empresa S.A. deve-se junto dos colaboradores envolvidos analisar o cenário pós vazamento e buscar as possibilidades de recuperação dos dados vazados e/ou dos danos morais causados ao cliente e a própria organização. Aqui é importante que através de reuniões regulares a equipe

envolvida possa minimizar ao máximo as perdas do valor da empresa e os dados do cliente e/ou empresa afetados.
>Exemplo:
Passado o período de emergência, Jorge Rodrigues deve tomar a frente da restauração do computador do cliente N2031, seguindo estritamente as orientações de configuração e manejo do Backup feitas por Matheus Martins, este que decidiu juntamente de Arthur Morais os procedimentos de restauração da máquina formatada. Arthur, realiza junto de Giovana Castro e Matheus Martins uma reunião para elaboração de novas práticas de infraestrutura para toda a equipe de Suporte, visando melhorar o manejo dos dados e decições em hora de crise.

Pós-incidente:
>Diretriz:
Apesar de medidas já terem sido tomadas durante a resposta ao incidente de segurança, é de extrema importância para a Empresa S.A. que o time de SI juntamente com os envolvidos no incidente discutam e apliquem rotineiramente correções e fortalecimentos para os sistemas de acordo com as vulnerabilidades e dados estudados e analisados durante o incidente. Recomenda-se que após o incidente e definição de novas politicas de segurança da informação a elaboração de reuniões gerais informativas pela Empresa S.A. e que seja atualizado as diretrizes de consentimentos dos clientes de acordo com essas leis.
>Exemplo:
Controlada a situação, Arthur Morais organizará o monitoramento regular da rede da Empresa S.A. (com destaque para o ramal da sala de manutenção de Notebook) que através de 1 reunião semanal com os times envolvidos no incidente, mostrara o desenrolar das novas medidas tomadas. Juntamente com a preocupação interna o time de Suporte oferecerá um monitoramento diário de segurança ao cliente N2031 no próximo mês, afim de manter sua fidelidade.

Motivos:
Cada integrante fictício foi escolhido baseado no que se espera de competências HardSkill e SoftSkill dos respectivos cargos: espera-se que um técnico de suporte saiba operar funções de manutenção e monitoramento de computadores tendo pensamento rápido para a solução de problemas; espera-se que um analista de suporte possua um capacidade analítica alta para perceber padrões incomuns unida a uma fala gentil para com o cliente; espera-se que um técnico de segurança da informação tenha capacidades por meio de ferramentas ou não de reconhecer cybervírus e lidar com elas, além de comunicar com a equipe; espera-se que um técnico de infraestrutura saiba manipular o trafeco dentro de um rede local, controlando permissões e passagens, mantendo a calma e organização para não afetar toda a infraestutura; espera-se que um gestor de departamento saiba quem atribuir para cada atividade em uma crise, buscando a qualidade e eficiência, mantendo a calma e praticidade.