The International Investment Funds Association
L'Association internationale des fonds d'investissement

ANBIMA

NOÇÕES BÁSICAS SOBRE O PROGRAMA DE SEGURANÇA CIBERNÉTICA

Defina um modelo – Um modelo de segurança cibernética (cybersecurity em inglês) é muito parecido com um conjunto de orientações. Ele ajuda a identificar o leque de informações a serem protegidas e fornece padrões, diretrizes e melhores práticas para a gestão da segurança cibernética relacionada aos riscos. Há vários modelos amplamente reconhecidos e eficazes que estabelecem um processo para a criação de controles efetivos via metodologias padronizadas de baixos custos e que promovem a proteção e solidez dos sistemas. No entanto, isso não significa que uma empresa precisa tomar como referência apenas um modelo. Usar partes de modelos diferentes que sejam mais apropriados para a sua companhia é algo que também pode ser eficaz.

Fontes adicionais:

https://www.nist.gov/cyberframework

https://www.iso.org/isoiec-27001-information-security.html

http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

https://www.cisecurity.org/controls/

Realize treinamentos de conscientização de segurança – O quadro de funcionários interage com os clientes, colegas, prestadores de serviços terceirizados e outros que são o "fator humano", tão frequentemente explorado pelos agressores (hackers). Uma defesa eficiente contra aqueles que querem se aproveitar de seus funcionários são os treinamentos de conscientização de segurança. Para esses treinamentos terem o máximo impacto, eles precisam ser contínuos, envolventes e testados em intervalos aleatórios. Ajudar os funcionários a avaliar as áreas que os hackers poderão tentar usar (no trabalho e em suas vidas pessoais), aplicando golpes como spams, phishing, engenharia social, ransomware e outros, contribuirá para reduzir o sucesso desses ataques.

Fontes adicionais:

https://resources.infosecinstitute.com/components-successful-security-awarenessprogram/#gref

https://www.sans.org/security-awareness-training

Tenha um Plano de Resposta a Incidentes – Um plano de resposta a incidentes é um conjunto de instruções que ajudam os funcionários a detectar, responder e se recuperar de incidentes de segurança das redes. Ele fornece um plano de ação para todos os incidentes significativos (que precisam ser definidos pelas empresas). Quando um contratempo significativo ocorre, sua empresa precisa de um plano de respostas a incidentes completo e detalhado, para ajudar os funcionários a interromper, conter e controlar rapidamente o incidente. Uma ameaça a uma organização, seja ela virtual ou física, pode ser incapacitante e um plano de respostas a incidentes pode ajudar a amenizar e preparar a empresa para uma série de eventos. O plano de resposta a incidentes deve ser testado e atualizado regularmente.

Fontes adicionais:

https://www.ibm.com/downloads/cas/PY31LRX2

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IncidentManagement-and-Response.aspx

Realize exercícios teóricos – Um plano de resposta a incidentes bem pensado que fica parado e não é exercido ou atualizado, não está cumprindo o seu objetivo. Os planos de respostas a incidentes precisam ser testados para que falhas sejam identificadas, mudanças sejam feitas e estratégias de atenuação aprovadas. Do mesmo modo, membros da equipe de funcionários precisam estar confortáveis com suas funções e responsabilidades durante um incidente cibernético grave. Como muitas empreitadas, é preciso ter prática.

Assumindo que você já identificou os participantes certos, quando da realização de um exercício teórico, você vai querer em primeiro lugar estabelecer uma série de objetivos em torno da extensão do cenário que você vai simular – por exemplo, um ataque distribuído de negação de serviço – e detalhar o grau de complexidade que você quer para o exercício. Você também deve estabelecer objetivos separados para o que pretende conseguir com o teste. Por exemplo, com que eficácia as políticas e procedimentos existentes são elaborados para responder a uma ameaça, e se as informações para contato estão atualizadas. Na medida em que sua empresa percorre o cenário, o exercício vai fornecer uma oportunidade de validação destas e outras informações. É importante que alguém documente as conclusões, para que eventuais falhas nos procedimentos possam ser resolvidas da maneira apropriada.

Fontes adicionais:

https://www.cisecurity.org/white-papers/six-tabletop-exercises-prepare-cybersecurityteam/

https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exerciseplaybook.pdf

Estabeleça e monitore atividades normais de rede – A atividade normal de rede diz respeito tanto aos funcionários quanto às redes. É prudente estabelecer um parâmetro para a rede normal e o comportamento dos funcionários. Certifique-se de que os funcionários somente terão acesso às partes da rede de que eles precisam para cumprir suas funções, saibam quais endereços IP podem se comunicar (ou geralmente se comunicam) com a sua rede, e saibam o que são os períodos de maior e menor tráfego. Entender e monitorar a atividade normal de rede vai ajudá-los a identificar anomalias que devem ser investigadas.

Fontes adicionais:

https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/monitoring

Participe do compartilhamento de informações confiáveis – As ameaças à segurança cibernética que todos enfrentamos são um "risco de proximidade" (neighborhood risk). Em outras palavras, estamos nessa juntos e desse modo somos mais fortes juntos. Formar redes ou comunidades de pares é um bom ponto de partida para os funcionários com responsabilidades de segurança cibernética, para que eles se conectem com outros que enfrentam os mesmos riscos. As redes informais, como o compartilhamento de informações não competitivas sobre vulnerabilidades e ameaças, são uma boa maneira de os funcionários de diferentes empresas adquirirem confiança. A troca de informações funciona melhor quando há o componente da confiança entre os participantes.

Fontes adicionais:

https://www.fsisac.com/

https://en.wikipedia.org/wiki/Computer_emergency_response_