NOÇÕES BÁSICAS DO PROGRAMA COMPLEMENTAR DE SEGURANÇA CIBERNÉTICA

Planejamento da Continuidade do Negócio - Em grande parte, uma área de concentração separada da área de segurança da informação, seu papel crítico e sua justaposição com ações de preparação para a segurança cibernética têm sido destacados durante a pandemia global de 2020. Normalmente, o planejamento para continuidade do negócio costumava se concentrar em interrupções operacionais de período relativamente curto, provendo estratégias voltadas a minimizar o impacto das interrupções para a empresa e para seus clientes. Durante 2020, o foco mudou, principalmente para contemplar interrupções de grande escala (global), trabalho remoto de longo prazo e o retorno, com segurança, dos funcionários aos escritórios. Os eventos de 2020 mudarão permanentemente o planejamento da continuidade do negócio das empresas.

Fontes adicionais:

https://www.continuitycentral.com/

https://www.thebci.org/

https://continuityinsights.com/

Controles de Tecnologia da Informação (TI) - Normalmente, formam um subconjunto dos controles internos de uma empresa, mas dizem respeito a atividades específicas, realizadas por pessoas ou por sistemas projetados para garantir que os objetivos do negócio sejam alcançados. No momento em que centenas de milhares de funcionários, em todo o mundo, foram orientados a trabalhar remotamente, os controles de TI tiveram que ser monitorados com mais rigor, na medida em que o cenário de ameaças se expandia drasticamente. Especificamente, a mudança referida acima acarretou maiores ameaças e riscos, que, por sua vez, causaram mudanças nos requisitos de controle.

Fontes adicionais:

https://www.isaca.org/resources/cobit

https://www.coso.org/Pages/default.aspx

Inventário e Controle de Software e de Hardware - Ações para combater a chamada "Shadow IT" (IT nas sombras), dentro da qual a tecnologia, o hardware e os aplicativos são configurados dentro de uma empresa sem aprovação ou sem a consciência de que podem significar novos riscos (por exemplo, falta de segurança, perda de dados, etc.), ineficiências e problemas de compatibilidade. Além disso, o acesso inadequado ou ilegítimo a sistemas e dados pode, no mínimo, afetar a integridade dos dados e a conformidade com regulamentos como o GDPR (General Data Protection Regulation) (Regulamento Geral sobre a Proteção de Dados, em

Português).

Additional Resources:

Fontes adicionais:

https://www.cisecurity.org/ https://www.asd.gov.au/

https://www.csoonline.com/article/3083775/shadow-it-mitigating-security-risks.html

Princípio do Menor Privilégio - Todo processo, usuário ou programa deve acessar apenas as informações e recursos necessários para serem usados de forma legítima. Segmentação da rede, com base na classificação dos dados armazenados em servidores, bem como localização separada de dados críticos ou sensíveis. Isso deve também incorporar um programa de prevenção de perda de dados que abranja pessoas, processos e sistemas, e que monitore e proteja os dados, estejam eles em uso, em movimento ou em repouso.

Fontes adicionais:

https://www.cisecurity.org/ https://nvd.nist.gov/800-53/Rev4/control/AC-6

https://www.sans.org/webcasts/design-privilege-architecture-aws-112925

Considerações sobre o Trabalho em Casa - Em algum momento durante a pandemia global de 2020, a maioria de nós foi orientada a trabalhar em casa. Embora, para fins de continuidade do negócio, isso tenha se mostrado eficaz, existem algumas preocupações de segurança, pois o 'escritório em casa' é um ambiente desconhecido. Algumas sugestões para ajudar a gerenciar os temas de segurança incluem: certificar-se de que um dispositivo corporativo seja usado para fins do negócio, conecte-se à empresa por meio de uma rede privada virtual, forneça proteção ao Wi-Fi doméstico, atualize o firmware do roteador ou substitua o roteador (se necessário), e implemente autenticação em dois fatores, entre outras ações.

Fontes adicionais:

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/working-from- home-here-s-what-you-need-for-a-secure-setup

Computerworld

https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home

Configuração Segura - Normalmente, quando um indivíduo (ou uma empresa) adquire um dispositivo, ele é configurado tendo em vista a facilidade de uso, em vez da segurança. O dispositivo chegará com configurações padrão, software desatualizado ou desnecessário, serviços habilitados / abertos, etc. A configuração segura do dispositivo é um processo, pois o software deteriora e as configurações são alteradas, e tal processo deve, portanto, ser gerenciado de forma contínua. A omissão desta etapa permitirá que invasores explorem serviços e software.

Fontes adicionais:

https://www.cisecurity.org/ https://www.itgovernance.co.uk/secure-configuration

https://www.nist.gov/news-events/news/2019/10/guide-security-focused-configuration-management-information-systems-nist