

SEGURANÇA CIBERNÉTICA

para clientes e usuários

Dez, 2023

Este material visa atender à Resolução CMN nº 4.893 de 26/2/2021.

A segurança abrange etapas de proteção que uma organização necessita para se manter segura contra ataques por meio de vulnerabilidades em sua infraestrutura física e lógica e que cada vez mais exige uma cooperação entre instituições financeiras e seus clientes.

O BNY Mellon entende que o programa de segurança da informação e cibersegurança de uma empresa é um processo contínuo e, portanto, visa fornecer o máximo de segurança possível para os produtos e serviços oferecidos, e contamos com a sua adoção de controles de segurança de informação e cibersegurança para o uso de dados, produtos e serviços que sustentam a parceria.

10 Boas Práticas no mundo digital

Dica 01: Defina um processo de classificação da informação, onde os dados da empresa recebam níveis de criticidade, para que os devidos critérios de acesso, retenção, manuseio, transferências e descarte sejam definidos e seguidos apropriadamente, garantindo a proteção durante o tempo de vida dos dados.

Dica 02: Certifique-se de que todos os usuários recebam conteúdo de conscientização e treinamentos periódicos e atualizados sobre Segurança da Informação e Cibersegurança. Treine seus usuários para identificarem ameaças cibernéticas. *#superdica**

Dica 03: Todos os usuários devem ser identificados por meio de login único, pessoal e intransferível e possuir somente os acessos necessários às suas funções, garantindo o critério de menor privilégio.

Dica 04: Utilize critérios de senha forte, reforce a ativação de autenticação de dois fatores (2FA) ou de autenticação de múltiplo fatores (MFA). Ao criar senhas seguras, você pode utilizar o conceito de senha forte e frases senhas. *#superdica**

Dica 05: Mantenha backups dos dados atualizados e um plano de continuidade de negócios que considerem processos, pessoas e tecnologia apropriado para o seu negócio.

Dica 06: Garanta que os softwares e dispositivos (incluindo os móveis) da sua empresa estejam com versões atualizadas. Todos os dispositivos devem ser protegidos com senha e ou criptografados. *#superdica**

Dica 07: Evite acessar a rede corporativa ou Internet utilizando wi-fi público. Use uma conexão de VPN ("Virtual Private Network" ou Rede Virtual Privada). *#superdica**

Dica 08: Utilize recursos de proteção contra vírus e ameaças virtuais, e mantenha-os atualizados. *#superdica**

Dica 09: Fique ciente de que a comunicação por e-mail pode ser insegura e fácil de falsificar. O e-mail de um conhecido ou até mesmo empresa com quem você tem negócios pode ser falso e criado para induzi-lo a fornecer dados pessoais ou até instalar softwares perigosos. *#superdica**

Dica 10: Realize auditorias em sua rede e corrija todos os pontos relacionados à segurança. Considere também os sistemas operacionais para identificar e eliminar possíveis vulnerabilidades e finalmente, use soluções de monitoramento, análise a detecção do tráfego de rede para se proteger de ciberataques.

Conheça as principais ameaças de Cibersegurança

Malware é um software malicioso capaz de monitorar o que o usuário está acessando ou digitando. Os primeiros malwares era conhecidos como vírus, mas agora o termo abrange tipos mais graves, como worms, cavalos de troia, spyware, adware, rootkits, botnets e ransomware.

Trojan é um tipo de malware que fica escondido em aplicativos ou programas, e que escondem funcionalidades mal intencionadas que alteram o sistema operacional do laptop ou celular para permitir ataques de criminosos.

DDoS é abreviação para **Ataque Distribuído de Negação de Serviço** que é uma sobrecarga de acessos ou tentativas de acessos à servidores sem necessariamente ser uma invasão. Esta sobrecarga gera instabilidade ou derruba temporariamente sites e ou serviços.

Ransomware é um tipo de código malicioso que bloqueia seu computador até que você pague um resgate para voltar a ter acesso aos seus dados. O pagamento do resgate geralmente é feito via bitcoins. O ransomware pode se propagar através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link ou explorando vulnerabilidades em sistemas desatualizado.

Clickjacking é um tipo de exploração online, em que os hackers induzem o usuário a clicar em algo diferente do que o usuário enxerga, potencialmente revelando informações confidenciais ou assumindo o controle de seu computador enquanto o usuário clica em páginas web aparentemente inofensivas.

Keylogging é uma ameaça geralmente ativada através de um software escondido que opera e registra o conteúdo que é digitado pelo teclado em um computador (da vítima). Informações como: login, senhas, mensagens, e-mails são gravados e enviadas para um servidor externo (para acesso do atacante).

Engenharia Social é uma abordagem não-tecnológica em que os criminosos utilizam informações que os próprios usuários publicam na Internet (redes sociais) ou verbalizam em locais públicos, para criar cenários e abordagens que viabilizam o crime.

Phishing é caracterizado por mensagens de e-mail falsa, de uma fonte aparentemente confiável ou respeitável, criada para induzir o usuário a clicar em um link ou abrir um arquivo não solicitado ou esperado. Uma vez que o usuário clica ou abre o arquivo, um software ou código é instalado no computador da vítima.

Spear Phishing é uma forma direcionada de phishing. Trata-se de e-mails fraudulentos que têm como alvo, pessoas, grupos ou empresas específicas com o objetivo de obter acesso a informações confidenciais.

Whaling Phishing é uma forma direcionada de phishing em que os criminosos usam para se disfarçar como se fosse um executivo ou funcionário em posições de influência dentro de uma empresa para obter informações ou acesso à sistemas da empresa.

Crime Cibernético é qualquer crime cometido eletronicamente, isso pode incluir roubo, fraude e às vezes até assassinato. Ex: roubo de identidade, materiais de abuso sexual infantil, roubo financeiro e violações de propriedade intelectual.

Gerenciamento de Incidente de Segurança Cibernética é um processo para identificar, gerenciar, registrar e analisar eventos e ameaças, que pode evitar ou mitigar os danos de um ataque cibernético. É importante que uma empresa tenha um processo em vigor para gerenciar e relatar eventos ou cenários que comprometam a confidencialidade, integridade ou disponibilidade das informações. Como boas práticas de gerenciamento, os incidentes devem ser identificados, documentados, respondidos, contidos e acompanhados visando atender, e não se limitar, as seguintes sugestões:

- 01** Estabelecer um registro do evento para manter as partes interessadas relevantes informadas, incluindo e não se limitando às equipes internas, reguladores, agências, mídia, regulador do setor, clientes, fornecedores e parceiros.
- 02** Especifique as informações necessárias para auxiliar no gerenciamento do incidente, como logs, configuração de rede e tipos, e níveis de informações e considere ferramentas para auxiliar no gerenciamento do incidente, como software de rastreamento e análise especializado.
- 03** A gestão e resposta à incidentes podem ser realizados internamente, ou considere ter um parceiro externo especializado para assumir o controle do processo quando necessário.

Lembre-se de que, dependendo da natureza de sua organização ou de seus clientes e parceiros, e das informações comprometidas, pode ser necessário relatar o incidente para várias autoridades, como, Banco Central do Brasil ou seu próprio regulador do setor e demais órgãos competentes.

Contato

Se você receber um e-mail do BNY Mellon suspeito ou que acredita ser fraudulento, entre em contato através dos canais oficiais disponíveis no [website](#)

Referências

NIST Cybersecurity Framework
Norma ISO/IEC 27001 (ISO 27001)

**Pratique na sua vida pessoal*