RENNÓ E MACHADO

ADVOGADOS ASSOCIADOS

OBJETIVOS DE SEGURANÇA CIBERNÉTICA

Setembro / 2024

Sumário

CONTROLE DE ATUALIZAÇÕES

Os Objetivos de Segurança Cibernética devem ser atualizados sempre que uma mudança, abrangendo funcionalidades que suportam as operações do RENNÓ E MACHADO for realizada, para assegurar que as alterações significativas se incorporem corretamente.

O "CSI – Comitê de Segurança da Informação" é responsável pelo desenvolvimento, implementação e manutenção deste plano.

Qualquer mudança significativa no procedimento deve ser analisada a relevância quanto a disponibilizar, informar e treinar se necessário, todos os envolvidos e todo o escritório.

Versão (Atualização)	Data	Necessidade	Responsável(eis)	Aprovado por
1.0	28/03/2024	Desenvolvimento do PCN	Maria Teresa Vinhas	André Rennó Breiner Machado
1.1	25/09/24	Revisão e atualização anual das Políticas Rennó e Machado.	DPO - Maria Teresa Vinhas	André Rennó Breiner Machado

CONTROLE DE CÓPIAS

Todos os envolvidos são responsáveis por manter uma cópia dos documentos conforme a seguir:

- Uma publicação completa estará disponível em PDF (Acrobat Reader) no One Drive (Serviço Microsoft de Nuvem) do RENNÓ E MACHADO.
- A cópia editável em DOCX (Microsoft Word) fica sob custódia dos Sócios Titulares e DPO.
- Este documento é classificado como CONFIDÊNCIAL E DE USO INTERNO e para sua publicação externa é necessário a autorização expressa do responsável pelos Sócios Titulares do RENNÓ E MACHADO.

OBJETIVOS DE SEGURANÇA CIBERNÉTICA

RENNÓ E MACHADO

1. Objetivos de Segurança Cibernética

Os objetivos de segurança cibernética do RENNÓ E MACHADO estão voltados a implementação, monitoramento e melhoria continua de procedimentos e controles para reduzir a vulnerabilidade da instituição a incidente e continuidade de negócios, realizando controles específicos, incluindo os voltados para a rastreabilidade da informação, buscando a segurança das informações sensíveis com foco na confidencialidade, integridade e disponibilidade, registrando a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para todas as atividades relacionadas.

Nossa área de Tecnologia da Informação do escritório utiliza as melhores práticas em segurança e continuidade para os seguintes procedimentos e controles para segurança cibernética, com a capacidade em **prevenir, detectar e reduzir** a vulnerabilidade a incidentes:

1.1. Autenticação

- Todos os usuários autorizados do RENNÓ E MACHADO, devem receber suas credenciais de acessos mediante ao conhecimento da política de segurança da informação e cibernética e política de continuidade de negócios.

- Não disponibilizamos acesso a clientes, portanto não temos a necessidade de uso de autenticação SHA - (Secure Hash Algorithm) ou "algoritmo de dispersão seguro".

- Todas as páginas e serviços de nossos ambientes na internet utilizam HTTPS (Hyper Text Transfer Protocol Secure - protocolo de transferência de hipertexto seguro), uma implementação que funciona como uma camada adicional de segurança. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais.

1.2. Criptografia

- Não disponibilizamos acesso a clientes, ou qualquer outro serviço.

- Não armazenamos dados de clientes em equipamentos móveis ou notebooks.

- Os sistemas criptográficos adotados em nossos ambientes, utilizam algoritmos e métodos eficazes anti-hacker, protegendo os ambientes de softwares maliciosos e acesso não autorizado, através de antivírus e antispam.

1.3. Prevenção e a detecção de intrusão

- Nosso ambiente utiliza "Firewall" para inspecionar pacotes e tráfego de dados, nas informações associadas a todas as camadas da rede e no estado das conexões e sessões ativas, com funções de prevenção de intrusão para identificar possíveis abusos dos protocolos de rede, mesmo em conexões aparentemente legítimas.

- Utilizamos ainda em nossos Firewalls as técnicas de IPS - Intrusion Prevention System (Sistema de Prevenção de Intrusão) e IDS – Intrusion Detection System (Sistema de Detecção de Intrusão), estes sistemas de prevenção e detecção de intrusão são capazes de distinguir entre um comportamento normal ou anormal do sistema.

- O tráfego de dados de nosso ambiente de rede é monitorado, um serviço que identifica as atividades maliciosas e aplicando as últimas definições de assinaturas e análise de comportamento, gerando informações de log sobre estas atividades, bem como o bloqueio ou a interrupção das mesmas.

- Nosso provedor de serviços, analisa toda atividade suspeita e ações são tomadas para minimizar ainda mais e proteger nossos ambientes.

1.4. Prevenção de vazamento de informações

- Possuímos controles e políticas que previnem o vazamento de informações, estabelecendo boas práticas no uso de correio eletrônico, acesso à internet, telefonia, análise comportamental dos funcionários, prestadores de serviços e na troca de informações com fornecedores.

- Nossas políticas de segurança da informação e cibernética e da continuidade de negócios, reforçam a cada colaborador a necessidade de se manter um ambiente que preze pela confidencialidade, disponibilidade e integridade das informações internas e de nossos clientes.

1.5. Realização periódica de testes e varreduras para detecção de vulnerabilidades

- Análises periódicas de testes e varreduras para detecção de vulnerabilidade, são realizadas somente no Firewall, uma vez que não temos sistemas ou aplicações na internet ou para acesso de clientes.

- Para prevenir nossos ambientes quanto as mais diversas vulnerabilidades, utilizamos soluções complementares que auxiliam na varredura e detecção de vulnerabilidades:

    - Procedimentos Internos (Políticas de segurança da informação e cibernética);
    - Atualizações de Segurança das estações, servidores e dispositivos de rede;
    - Instalação de antivírus contra ameaças maliciosas e intencionais;
    - Firewalls e Filtros de Conteúdo protegendo e monitorando todo o ambiente.

1.6. Proteção contra softwares maliciosos

Executamos os procedimentos necessários para que softwares maliciosos não cheguem a nível da rede:

Proteção especializada contra Malwares

Para proteção contra softwares maliciosos, utilizamos Antivírus Corporativo, para evitar danos causados em arquivos, sistemas ou rede de computadores, afetando negócios e reputação do RENNÓ E MACHADO com capturas de informações ou utilização de nossos equipamentos para ações ilícitas.

A Política de Segurança da Informação do RENNÓ E MACHADO contém diretrizes para prevenir ação de software maliciosos.

Quanto a **recuperação em caso de incidente, os procedimentos contidos no plano de contingência devem ser utilizados para minimizar os danos**.

Todas as diretrizes na política têm como objetivo atender aos seguintes tipos de malware:

- **Adware**
  Exibe publicidade indesejada e às vezes maliciosa na tela de um computador ou dispositivo móvel, redireciona os resultados da pesquisa para sites de publicidade e captura os dados do usuário que podem ser vendidos para anunciantes sem o consentimento do usuário.
- **Spyware**
  Se esconde no dispositivo e monitora atividades e rouba informações sensíveis como dados financeiros, informações de conta, logins e muito mais. Spyware pode se espalhar explorando vulnerabilidades de softwares ou então ser empacotado com software legítimo ou em Trojans.
- **Ransomware**
  Malware com foco em bloquear usuários fora de seu sistema ou negar acesso aos dados até que um resgate seja pago.
- **Crypto-malware**
  Tipo de ransomware que criptografa arquivos de usuários e requer pagamento em um prazo específico e muitas vezes através de uma moeda digital como o Bitcoin.
- **Cavalos de Tróia ou Trojans**
  Disfarça-se de software legítimo para enganar o usuário na execução de software malicioso no seu computador. Uma vez instalado um Trojan em um dispositivo, os hackers podem usá-lo para apagar, modificar ou capturar dados, coletar o dispositivo como parte de uma botnet, espionar o dispositivo ou obter acesso à sua rede.
- **Worms**
  Explora as vulnerabilidades do sistema operacional a partir de uma rede e se replica para infectar outros computadores sem exigir ação de ninguém.
- **Vírus**
  Pedaço de código que se insere em um aplicativo e é executado quando o aplicativo é executado. Uma vez dentro de uma rede, um vírus pode ser usado para roubar dados sensíveis, lançar ataques DDoS ou conduzir ataques de ransomware.
- **Keyloggers**
  Tipo de spyware que monitora a atividade do usuário e podem ser usados para roubar dados de senha, informações bancárias e outras informações sensíveis. Keyloggers podem ser inseridos em um sistema através de phishing, engenharia social, ou downloads maliciosos.
- **Bots e botnets**
  Um bot é um computador que foi infectado com malware e uma coleção de bots chamada botnet. Os botnets ou rede de bots podem incluir milhões de dispositivos à medida que se espalham sem serem detectados. Botnets ajudam

hackers com inúmeras atividades maliciosas, incluindo ataques DDoS, envio de spam e mensagens de phishing, e propagação de outros tipos de malware.

- **Malware PUP**
  PUPs— 'programas potencialmente indesejáveis', na sigla em inglês, são programas que podem incluir publicidade, barras de ferramentas e pop-ups que não estão relacionados com o software que você baixou.

- **Híbridos**
  A maioria dos malwares são uma combinação de diferentes tipos de softwares maliciosos, muitas vezes incluindo partes de Trojans e worms e, ocasionalmente, um vírus.

- **Malwares sem arquivos**
  Tipo de software malicioso que utiliza programas legítimos para infectar um computador. Ele não depende de arquivos e não deixa pegada, o que torna difícil detectar e remover. Sem ser armazenado em um arquivo ou instalado diretamente em uma máquina, as infecções sem arquivos vão direto para a memória e o conteúdo malicioso nunca toca no disco rígido.

- **Bombas lógicas**
  Tipo de malware que só se ativa quando acionado, como em uma data e hora específica ou no 20º logon em uma conta. Vírus e worms muitas vezes contêm bombas lógicas para entregar seu código malicioso em um momento pré-definido ou quando outra condição é satisfeita.

Fonte: www.kaspersky.com.br/resource-center/threats/types-of-malware

1.7. Estabelecimento de mecanismos de rastreabilidade

Os equipamentos de rede e servidores do RENNÓ E MACHADO entendidos como estratégicos, geram LOG/Registro para auxiliar na rastreabilidade de anomalias, eventos e vulnerabilidades em nossos ambientes.

2. Manutenção de cópias de segurança dos dados e das informações

Utilizamos os seguintes controles:

a. Os backups realizados pelos usuários devem ser mantidos na nuvem (One Drive), para livrá-los de qualquer dano que possa ocorrer na instalação principal;
b. Nosso ambiente em nuvem (OneDrive), recebem um nível adequado de proteção física, compatível ou acima dos padrões utilizados no ambiente principal;
c. Não permitimos a utilização de backup em mídias removíveis, somente na nuvem.

Responsável Técnico:

Carlos Macedo
Executivo de Risco, Segurança e Tecnologia da Informação
Auditor Líder Certificado em Sistemas de Gestão de Continuidade de Negócios (BS25999) – BSI

carlos.macedo@irmc.com.br

IRMC Partners
www.irmc.com.br
São Paulo - SP

+55 11 4673 4774