ANAC AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

Manual de COMPARTILHAMENTO DE INFORMAÇÕES DE CIBERSEGURANÇA

MANUAL DE COMPARTILHAMENTO DE INFORMAÇÕES DE CIBERSEGURANÇA

COORDENAÇÃO TÉCNICA

Werllen Lauton Andrade (GTCF/GSEF/SIA/ANAC)

Sylvio José Coelho de Souza (CSCI/GTCF/GSEF/SIA/ANAC)

EQUIPE TÉCNICA RESPONSÁVEL

1S BET Leonardo Pereira Estevão	DECEA
1T ENG ELN Vitor Borges Coutinho da Silva	DECEA
Adriano Vieira Guimarães	GRU Airport
Cel Av R1 Leandro Costa de Andrade	DECEA
CP ENG CMP Tiago Porto Barbosa	DECEA
Cv Marcelo Cirelle Lucas de Melo	DECEA
Felipe Canosa	GRU Airport
Henrique Rogge Gomes	GRU Airport
Marco Aurelio Fontenelle Moreira	RIOGaleão
Marcus Batista	GRU Airport
Marcus Vinicius Ferreira dos Santos	EMBRAER
MJ Esp Com Marco Aurelio Sernagiotto	DECEA
Rafael Lima Prado	GRU Airport
Rosemberg André da Silva	ANAC
Sylvio José Coelho de Souza	ANAC
TC Eng ELN Cleiton Almeida Ataide	DECEA
Werllen Lauton Andrade	ANAC

DÚVIDAS, SUGESTÕES E CRÍTICAS PODEM SER ENVIADAS PARA O E-MAIL

cyber.sia@anac.gov.br

SUMÁRIO

INTRODUÇÃO

A colaboração entre diferentes organizações é fundamental para enfrentar os desafios crescentes no campo da cibersegurança. No setor de transporte aéreo, essa colaboração se torna ainda mais crucial devido à complexidade e à criticidade das operações envolvidas. O compartilhamento de informações de cibersegurança se consolida como a pedra angular dessa cultura colaborativa, permitindo que as organizações se antecipem a ameaças, mitiguem riscos e fortaleçam suas defesas coletivas.

Este manual é um exemplo concreto dessa colaboração. Desenvolvido no âmbito da 6ª Edição do Exercício Guardião Cibernético, ele contou com a participação conjunta de diversas entidades do setor de transporte aéreo, incluindo: Agência Nacional de Aviação Civil (ANAC), Departamento de Controle do Espaço Aéreo (DECEA), RIOGaleão, GRU Airport, EMBRAER.

A metodologia 5W2H foi utilizada na elaboração deste manual, garantindo uma abordagem estruturada e abrangente. Essa metodologia responde às seguintes perguntas:

- **What** (O que): O que é o compartilhamento de informações de cibersegurança.
- **Why** (Por quê): Por que compartilhar informações de cibersegurança.
- **When** (Quando): Quando compartilhar informações de cibersegurança.
- **Who** (Quem): Quem é responsável pelo compartilhamento de informações de cibersegurança.
- **Where** (Onde): Onde as informações de cibersegurança são compartilhadas.
- **How** (Como): Como as informações de cibersegurança são preparadas e compartilhadas.
- **How Much** (Quanto): Quanto custam os recursos dedicados ao compartilhamento de informações de cibersegurança.

Este manual é um documento em constante evolução, refletindo o compromisso contínuo das organizações participantes em aprimorar suas práticas de cibersegurança. Sugestões de melhorias são bem-vindas e podem ser enviadas para o e-mail: cyber.sia@anac.gov.br.

CAPÍTULO 1 - O QUE É O COMPARTILHAMENTO DE INFORMAÇÕES DE CIBERSEGURANÇA

Compartilhamento de informações de cibersegurança é o processo de troca de dados, relatórios, indicadores de ameaças, vulnerabilidades, e práticas de segurança entre organizações, governos, e indivíduos com o objetivo de aumentar a proteção contra ameaças cibernéticas.

Este processo pode ocorrer em diversas formas, como alertas de ameaças contendo Informações sobre novos tipos de *malware*, técnicas de ataque e vulnerabilidades conhecidas. Através de indicadores de comprometimento (IoCs) com dados técnicos que identificam atividades maliciosas, como endereços IP suspeitos, URLs maliciosos, *Hashes* de arquivos comprometidos, entre outros. Também consiste na divulgação de boas práticas de segurança através de recomendações sobre como configurar sistemas de forma mais segura ou implementar controles específicos para mitigar riscos.

Este tipo de colaboração permite que os participantes se antecipem a ataques cibernéticos, reduzam o impacto de incidentes e desenvolvam melhores estratégias de defesa.

O compartilhamento de informações é uma das ferramentas mais poderosas na luta contra ciberataques. Sua importância pode ser evidenciada pela detecção rápida de ameaças ao se compartilhar indicadores em tempo real. Uma organização que detecta um comportamento malicioso pode ajudar outras a identificar e bloquear ataques semelhantes antes que causem danos. Nenhuma organização, por maior ou mais avançada que seja, tem uma visão completa de todas as ameaças cibernéticas em tempo real. Através do compartilhamento, a inteligência sobre ameaças se torna mais ampla e eficaz. Uma organização que enfrenta um ataque pode compartilhar lições aprendidas e táticas de mitigação que ajudarão outras a evitar ou minimizar o impacto de ataques semelhantes. Compartilhar dados de incidentes permite a criação de padrões de resposta e a implementação de estratégias preventivas que aumentam a eficiência das operações de segurança. A cibersegurança afeta tanto organizações privadas quanto governos. O compartilhamento de informações em uma escala maior contribui para a segurança nacional, melhorando a defesa contra ataques que podem afetar infraestruturas críticas.

CAPÍTULO 2 - POR QUE COMPARTILHAR INFORMAÇÕES DE CIBERSEGURANÇA

Há uma série de razões estratégicas, operacionais e regulatórias para o compartilhamento de informações de cibersegurança. Estas razões não apenas beneficiam a organização que compartilha as informações, mas também o ecossistema de segurança como um todo.

A principal razão para compartilhar informações é a mitigação de riscos. O conhecimento compartilhado sobre ameaças, vulnerabilidades e soluções de mitigação permite que as organizações sejam mais proativas em sua defesa. Ao colaborar, as organizações podem adotar medidas preventivas e corretivas mais rapidamente, evitando que um ataque explorado em uma entidade se espalhe para outras.

Construir uma Cultura de Cooperação é essencial em cibersegurança. Organizações que compartilham informações demonstram um compromisso com o bem comum, promovendo um ambiente colaborativo. Isso é particularmente relevante em setores como saúde, finanças, e infraestrutura crítica, onde ataques cibernéticos podem ter consequências devastadoras.

Em alguns setores, o compartilhamento de informações de segurança cibernética não é apenas uma prática recomendada, mas uma obrigação regulatória. Governos e órgãos reguladores frequentemente exigem que empresas de setores críticos relatem incidentes de segurança e compartilhem informações com as autoridades para monitoramento e proteção nacional.

Exemplos de regulamentações incluem:

- LGPD (Lei Geral de Proteção de Dados): Lei que estabelece regras para o tratamento de dados pessoais, como a sua coleta, armazenamento, compartilhamento e uso, e que exigem a notificação aos órgãos competentes em caso de violações;
- GDPR (Regulamento Geral sobre a Proteção de Dados da União Europeia): Que impõe a notificação de violações de dados a autoridades de proteção de dados.

O compartilhamento de informações também fortalece a resiliência organizacional uma vez que a organização que adota essa prática se torna mais preparada para detectar, responder e se recuperar de incidentes cibernéticos. Ao aprender com as experiências de outras entidades, a organização consegue adaptar e melhorar suas próprias defesas.

Manter uma reputação sólida no mercado é fundamental, e organizações que falham em proteger seus dados ou que são vítimas de ataques cibernéticos frequentemente sofrem danos à sua marca e confiança do cliente. Compartilhar informações sobre ameaças e incidentes pode ajudar a minimizar o risco de ataques futuros, protegendo assim a reputação da empresa.

Ao adotar práticas colaborativas de compartilhamento, as organizações podem reduzir os custos operacionais associados à cibersegurança. Investir individualmente em inteligência de ameaças, ferramentas de monitoramento e equipes de resposta a incidentes pode ser dispendioso. No entanto, ao compartilhar informações, as organizações podem dividir os custos associados à coleta de inteligência e à defesa proativa, tornando suas operações mais eficientes financeiramente.

O compartilhamento de informações permite que as organizações se antecipem a novas ameaças. À medida que surgem novas técnicas de ataque e ferramentas maliciosas, as organizações que participam de redes de compartilhamento podem ser notificadas em tempo real sobre novos vetores de ataque e vulnerabilidades, possibilitando a adoção de medidas proativas antes que os ataques se concretizem.

Em resumo, compartilhar informações de cibersegurança é crucial para proteger sistemas e dados contra ameaças. Isso pode ser feito por meio de:

1. **Detecção de Vulnerabilidades**: Quando uma vulnerabilidade é descoberta em um sistema ou software, é importante compartilhar essa informação com os desenvolvedores e usuários para que possam tomar medidas corretivas.

2. **Incidentes de Segurança**: Se um incidente de segurança ocorrer, como um ataque cibernético, compartilhar detalhes sobre o incidente pode ajudar outras organizações a se protegerem contra ameaças semelhantes.

3. **Atualizações e Patches**: Informar os usuários sobre atualizações e patches de segurança é essencial para garantir que todos estejam protegidos contra vulnerabilidades conhecidas.

4. **Colaboração com CERTs/CSIRTs**: Compartilhar informações com equipes de resposta a emergências cibernéticas (CERTs/CSIRTs) pode ajudar na coordenação de respostas a incidentes e na mitigação de ameaças em larga escala.

5. **Educação e Conscientização**: Compartilhar boas práticas e informações sobre ameaças emergentes pode aumentar a conscientização e a preparação geral contra ataques cibernéticos.

CAPÍTULO 3 - QUANDO SE COMPARTILHAM INFORMAÇÕES DE CIBERSEGURANÇA

Diferentemente dos reportes, em que o envio de informações a uma autoridade é obrigatório nas hipóteses previstas em regulação, no caso do compartilhamento de informações de cibersegurança, não há uma descrição exaustiva das situações em que deve ou não ocorrer. Cabe a cada pessoa e organização definir a pertinência e relevância de compartilhar uma informação de segurança cibernética, bem como a quem enviá-la.

O compartilhamento de informações de cibersegurança é uma prática essencial para aumentar a resiliência do setor contra ataques cibernéticos, sendo incentivada entre todas as organizações do setor. Deve ocorrer sempre que uma instituição identificar fragilidades ou possíveis incidentes de segurança que possam afetar outras instituições. Compartilhar informações rapidamente pode ajudar outras organizações a se protegerem, preservando a confidencialidade, integridade e disponibilidade dos dados e sistemas, além de beneficiar a continuidade dos negócios.

Recomenda-se compartilhar informações de cibersegurança nas seguintes situações:

- Sempre que um incidente de cibersegurança for detectado, é crucial compartilhar informações imediatamente com todas as partes interessadas relevantes, incluindo pessoal interno e clientes.
- Regularmente, acerca de novas ameaças e vulnerabilidades identificadas, por meio de relatórios de inteligência de ameaças e atualizações de fornecedores.
- Após a mitigação de um incidente, compartilhar informações sobre as ações tomadas e lições aprendidas.
- Em caso de ameaças iminentes ou emergências de cibersegurança, por meio de alertas imediatos para todas as partes relevantes para permitir uma resposta rápida e coordenada.

Diversas outras situações podem demandar o compartilhamento de informações, cabendo às organizações e pessoas que as compõem definir quando compartilhar. Independentemente do caso, o tomador de decisão deve considerar a pertinência, confiabilidade, impacto potencial e necessidade de conhecimento das partes interessadas, garantindo sempre a confidencialidade e segurança das informações compartilhadas.

Além disso, plataformas de compartilhamento automatizado, como o MISP, podem agilizar esse processo ao aplicar regras pré-estabelecidas que facilitam o envio de informações para organizações com as quais já se estabeleceu uma relação de confiança. O MISP permite a coleta, armazenamento e compartilhamento de indicadores de comprometimento e outras informações de ameaças de forma estruturada e automatizada, promovendo uma colaboração eficiente e segura entre as partes interessadas.

CAPITULO 4 - QUEM É RESPONSÁVEL POR COMPARTILHAR INFORMAÇÕES DE CIBERSEGURANÇA

A responsabilidade pelo compartilhamento de informações de cibersegurança é dividida entre várias partes interessadas, visto que é baseada na colaboração:

1. **Agências Estatais**: Devem desenvolver e participar de parcerias e mecanismos de compartilhamento de informações sobre ameaças cibernéticas, incidentes, tendências e esforços de mitigação, tanto nacional quanto internacionalmente. Exemplos: Ministérios de Defesa, Agências de Segurança Nacional, Autoridades de Aviação Civil.

2. **Indústria da Aviação**: Devem colaborar e compartilhar informações relevantes para proteger a infraestrutura crítica da aviação. Exemplos: Operadores de aeronaves, aeroportos, provedores de serviços de navegação aérea, *Aviation ISAC (Comprises an international community of airlines, airports, IFE/Satcom, OEMs, and aviation service providers)*.

3. **CERTs/CSIRTs**: Equipes de resposta a emergências cibernéticas que coordenam e compartilham informações para mitigar ameaças em larga escala. Exemplos: CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), CSIRT de empresas e organizações, CTIR Gov (Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo), EATM-CERT do Eurocontrol (*European Air Traffic Management - Computer Emergency Response Team*).

4. **Organizações Internacionais**: Como a ICAO, que facilita a cooperação internacional e a harmonização dos esforços de cibersegurança na aviação.

O compartilhamento de informações de cibersegurança é uma responsabilidade dividida entre várias partes interessadas, incluindo agências estatais, a indústria da aviação, CERTs/CSIRTs, organizações internacionais e pesquisadores de segurança. A estruturação adequada das informações e a escolha dos métodos de compartilhamento são cruciais para garantir que as informações sejam úteis e acionáveis, contribuindo para a proteção coletiva contra ameaças cibernéticas.

CAPÍTULO 5 – POR QUE MEIOS SE COMPARTILHAM INFORMAÇÕES DE CIBERSEGURANÇA

O compartilhamento de informações de cibersegurança é essencial para prevenir e mitigar incidentes de segurança. Inicialmente feito de forma manual, através de relatórios e conferências, o processo evoluiu com o surgimento de plataformas automatizadas, como o MISP (*Malware Information Sharing Platform*), que facilita a troca de dados em tempo real sobre ameaças, vulnerabilidades e indicadores de comprometimento (IoCs). O objetivo deste texto é discutir os diferentes métodos de compartilhamento e sua evolução no campo da cibersegurança.

Historicamente, o compartilhamento de informações de segurança cibernética é feito por meios tradicionais de veiculação de informações, como relatórios, e-mails ou reuniões. Embora eficazes em alguns casos, esses métodos mostram-se lentos e propensos a erros em certas situações, em especial para veiculação de informações de segurança cibernética, dado o volume de interações e quantidade de informações técnicas envolvidas.

Com o aumento da complexidade e frequência dos ataques, tornou-se necessária uma solução mais ágil e precisa. Assim, surgiram as plataformas automatizadas, que permitem a troca de informações de forma estruturada e eficiente, reduzindo o tempo de resposta e melhorando a detecção de ameaças.

Abaixo serão trazidos alguns exemplos de meios para compartilhamento de informação de cibersegurança. Deve-se ter em mente que o tipo de plataforma a ser usado deve levar em consideração a natureza da informação a ser compartilhada, a classificação de sigilo, o grau de urgência e relevância entre outros fatores. Cabe ao interlocutor definir, com base na informação a ser passada, o meio mais adequado.

TELEFONE

O telefone continua a ser uma ferramenta essencial para situações críticas, especialmente em setores como aviação e saúde, onde respostas rápidas são cruciais. Por exemplo, no caso de uma falha catastrófica em um sistema de controle aéreo, o uso do telefone permite a transmissão direta de informações TLP:RED, garantindo que decisões sejam tomadas em tempo real. Entretanto, organizações já relataram tentativas de ataques via falsificação de voz utilizando IA destacando a necessidade de verificações robustas de identidade.

E-MAIL SIMPLES

Embora amplamente utilizado, o e-mail simples tem limitações práticas no mundo real. Em investigações de incidentes, analistas de segurança frequentemente enfrentam desafios com e-mails bloqueados por conterem Indicadores de Comprometimento (IoCs). Além disso, já houve casos em que informações classificadas como TLP:RED foram inadvertidamente enviadas para endereços genéricos, o que representou uma brecha de segurança significativa. Manter listas de e-mails atualizadas também é um desafio em organizações com alta rotatividade de funcionários.

E-MAIL COM ANEXO

O envio de anexos criptografados por e-mail é comum em setores financeiros, onde dados sensíveis sobre fraudes ou ataques cibernéticos precisam ser protegidos. No entanto, a revisão manual desses anexos pode atrasar a resposta a incidentes urgentes. Por exemplo, um banco relatou que o tempo de reação a uma ameaça foi prolongado porque a análise do anexo dependia da disponibilidade de especialistas, evidenciando a importância de automação em certos processos.

REPOSITÓRIO PRIVADO

Repositórios privados são amplamente utilizados por organizações que participam de parcerias de inteligência cibernética, como em comunidades financeiras e de infraestrutura crítica. Bancos e empresas de energia, por exemplo, utilizam esses repositórios para compartilhar dados de ameaças em tempo real com parceiros de confiança. Um estudo recente mostrou que repositórios bem geridos, com autenticação multifator e monitoramento rigoroso de acesso, reduziram significativamente o tempo para identificar e mitigar ataques. Porém, também há relatos de desafios na organização desses repositórios à medida que a quantidade de dados cresce, exigindo esforços constantes para mantê-los funcionais.

APLICATIVOS E PLATAFORMAS DE COMPARTILHAMENTO DE AMEAÇAS

Aplicações como o MISP têm sido usadas com sucesso por grandes empresas de telecomunicações para compartilhar rapidamente indicadores de comprometimento. Um exemplo prático envolve uma colaboração entre operadoras de telecomunicações que, através do MISP, conseguiram identificar e mitigar uma campanha de *phishing* massiva em questão de horas. Plataformas como o OpenCTI também são populares em instituições financeiras, automatizando o compartilhamento de inteligência sobre fraudes, reduzindo o esforço manual e acelerando as respostas a ameaças.

Plataformas como o MISP são particularmente eficazes em indústrias como a de tecnologia e defesa, onde o compartilhamento de informações sobre *malwares* e IoCs é essencial para uma rápida mitigação de riscos. Por exemplo, em uma cooperação internacional sobre cibersegurança, o MISP foi utilizado para compartilhar detalhes sobre uma nova variante de *ransomware*, permitindo que empresas em diferentes países implementassem defesas antes que fossem atacadas.

Conforme sítio eletrônico oficial (https://www.misp-project.org/features/), o MISP consiste em uma plataforma de inteligência de ameaças para compartilhar, armazenar e correlacionar Indicadores de Comprometimento de ataques direcionados, inteligência de ameaças, informações sobre fraudes financeiras, informações sobre vulnerabilidades ou até mesmo informações de contraterrorismo. Trata-se de uma ferramenta importante cuja utilização vem sendo cada vez mais incentivada até mesmo por órgãos do governo (https://www.gov.br/cisc/pt-br/etir-as-a-service/misp).

Este documento possui apêndice com um Guia de Instalação do MISP. Mais informações sobre a instalação, configuração e melhores práticas referentes a essa plataforma podem ser consultadas na página do CERT.BR, que promove workshops sobre o tema: https://www2.cert.br/misp/

REDES COLABORATIVAS E ISACS

Os ISACs (*Information Sharing and Analysis Centers*) têm sido cruciais para setores como o financeiro, saúde e energia, onde a troca de informações em tempo real pode prevenir grandes incidentes. Um exemplo notável ocorreu no setor financeiro, onde o FS-ISAC (*Financial Services ISAC*) compartilhou detalhes de um ataque cibernético massivo a bancos nos EUA, o que permitiu a implementação de defesas preventivas em instituições de outros países. A colaboração intersetorial via ISACs tem se mostrado uma prática essencial na defesa de infraestruturas críticas.

CAPÍTULO 6 – COMO AS INFORMAÇÕES DE CIBERSEGURANÇA SÃO PREPARADAS PARA O COMPARTILHAMENTO

A preparação das informações de cibersegurança para o compartilhamento envolve vários passos críticos que garantem que os dados sejam úteis e compreensíveis para os destinatários. Este capítulo aborda em detalhes os processos de avaliação, análise e aplicação do *Traffic Light Protocol* (TLP) nas informações a serem compartilhadas.

AVALIAÇÃO DA INFORMAÇÃO

A avaliação da informação é o primeiro passo para garantir que os dados coletados sejam relevantes e precisos. A avaliação deve incluir:

- **Avaliação da Confiabilidade**: Avalie a confiabilidade e a credibilidade da fonte da informação. Fontes confiáveis aumentam a integridade dos dados compartilhados.
- **Verificação da Precisão**: Confirme a exatidão dos dados através de fontes confiáveis e métodos de validação. Dados incorretos ou desatualizados podem levar a decisões erradas.
- **Identificação da Relevância**: Determine a importância da informação em relação ao contexto atual de cibersegurança. Pergunte-se se os dados são essenciais para os destinatários e se podem ajudá-los a tomar decisões informadas.
- **Urgência e Impacto Potencia**l: Avalie a informação acerca de sua urgência e impacto potencial. Informações críticas que requerem ação imediata e que podem ter um alto impacto na segurança da organização ou dos parceiros devem ser priorizadas no compartilhamento.

MARCAÇÃO TLP (TRAFFIC LIGHT PROTOCOL)

O *Traffic Light Protocol* (TLP) é um conjunto de designações usadas para indicar a sensibilidade da informação compartilhada e as restrições de disseminação. Foi desenvolvido pelo *Forum of Incident Response and Security Teams* (FIRST) para facilitar uma maior divulgação de informações sensíveis enquanto se controla a circulação e a distribuição. O TLP é essencial para garantir que as informações sejam compartilhadas de maneira responsável e segura.

O objetivo principal do TLP é fornecer uma linguagem comum para descrever como a informação pode ser compartilhada, garantindo ao mesmo tempo que a disseminação dessas informações ocorra de maneira controlada e apropriada. Isso ajuda as organizações a balancearem a necessidade de compartilhar informações cruciais com a proteção contra possíveis riscos associados à divulgação não controlada.

A utilização do TLP traz os seguintes benefícios para a informação:

- **Clareza na Comunicação**: O TLP oferece um sistema claro e padronizado para comunicar restrições de compartilhamento, facilitando a compreensão das diretrizes de disseminação.
- **Proteção da Informação**: O TLP ajuda a proteger informações sensíveis contra divulgação não autorizada ou inadvertida, reduzindo o risco de vazamentos de dados.
- **Confiabilidade e Segurança**: Ao usar o TLP, as organizações podem estabelecer uma relação de confiança com seus parceiros, sabendo que as informações serão tratadas de acordo com as diretrizes acordadas.
- **Facilitação da Colaboração**: O TLP promove a colaboração segura entre diferentes entidades, incluindo setores público e privado, permitindo uma resposta mais eficaz às ameaças cibernéticas.

VERSÃO 2.0 DO TLP

A partir de março de 2022, a versão 1.0 do TLP foi descontinuada e a versão 2.0 do TLP foi implementada. O TLP inclui as seguintes categorias:

TLP:RED Para uso estritamente limitado aos destinatários iniciais. Este nível é utilizado quando a divulgação da informação pode causar danos significativos se compartilhada com um público mais amplo. Destinatários não podem compartilhar informações TLP:RED com mais ninguém.

Cor: #FF2B2B
Fundo: #000000

TLP:AMBER+STRICT Utiliza-se quando é necessário apoio para agir com eficácia sobre a informação, mas existe risco para a privacidade, reputação ou operações das organizações envolvidas ao disseminar a informação. Neste caso as informações somente podem ser compartilhadas dentro da organização, com uma distribuição ainda mais restrita do que TLP:AMBER. Destina-se a informações altamente sensíveis que requerem um controle rigoroso.

Cor: #FFC000
Fundo: #000000

TLP:AMBER Utiliza-se quando é necessário apoio para agir com eficácia sobre a informação, mas existe risco para a privacidade, reputação ou operações das organizações envolvidas ao disseminar a informação. Neste caso as informações somente podem ser compartilhadas internamente dentro da organização e com seus clientes. Deve ser tratada com cautela e não deve ser compartilhada publicamente.

Cor: #FFC000
Fundo: #000000

TLP:GREEN Use esta marcação quando a informação for útil para conscientizar a nível de sua comunidade (no caso da aviação civil, pode ser disseminada entre várias organizações de diferentes níveis do setor). Compreende informações que podem ser compartilhadas com parceiros de negócios e dentro da comunidade de cibersegurança. Deve ser protegida, mas não possui restrições tão rígidas quanto as categorias anteriores. Não devem ser mantidas em canais publicamente acessíveis.

Cor: #33FF00
Fundo: #000000

TLP:CLEAR Esta marcação é utilizada para informações que podem ser compartilhadas publicamente sem restrições. É destinada à ampla disseminação e pode incluir boas práticas, alertas de segurança pública e outras informações de interesse geral.

Cor: #FFFFFF
Fundo: #000000

O TLP possui marcações específicas de cores de forma padronizada, as quais devem ser utilizadas sempre que possível. Essas cores foram desenvolvidas para atender às necessidades de pessoas com baixa visão.

A fonte da informação deve assegurar que os destinatários de uma informação com marcação TLP compreendam e sigam as diretrizes de compartilhamento. A fonte também pode determinar restrições adicionais de compartilhamento, as quais devem ser respeitadas pelos destinatários. Se um destinatário precisar compartilhar uma informação além do permitido pela marcação TLP original, ele deve obter permissão explícita da fonte.

O TLP foi estabelecido pelo *Forum of Incident Response and Security Teams* (FIRST). O CTIR GOV disponibiliza em sua página a versão traduzida para o português do referido documento, com mais detalhes e explicações. Para acessar, visite: CTIR GOV – TLP.

Consulte também a página do Centro Integrado de Segurança Cibernética do Governo Digital (CISC) sobre o assunto: Traffic Light Protocol (TLP) — Centro Integrado de Segurança Cibernética do Governo Digital (www.gov.br)

PREPARO PARA O COMPARTILHAMENTO

Finalmente, a informação precisa ser formatada e preparada para o compartilhamento. Este processo inclui:

- **Formatação Consistente**: Garanta que todos os dados sejam apresentados de maneira consistente e fácil de entender. Utilize padrões de formatação e estruturação que facilitem a leitura e a interpretação. Verifique se a marcação TLP está sendo utilizada adequadamente.

- **Contextualização**: Adicione contexto adicional onde necessário para ajudar os destinatários a compreenderem a relevância e o impacto da informação. Explique termos técnicos e forneça exemplos práticos.

- **Validação Final**: Realize uma verificação final dos dados antes do compartilhamento. Certifique-se de que todos os dados estejam corretos, completos e atualizados.

- **Distribuição Segura**: Utilize canais seguros para o compartilhamento das informações, garantindo que somente os destinatários autorizados tenham acesso.

CAPÍTULO 7 – QUANTO CUSTAM OS RECURSOS DEDICADOS AO COMPARTILHAMENTO DAS INFORMAÇÕES DE CIBERSEGURANÇA

O custo financeiro do compartilhamento de informações de cibersegurança deve ser adequadamente calculado, para se assegurar que estará apropriadamente previsto nas definições orçamentárias da organização, de modo a garantir a continuidade dessa atividade.

Antes de mais nada, é necessário compreender que os atos de proteção das informações sensíveis não são, em muitos casos, opcionais, mas sim devem ser realizados no cumprimento de obrigações regulamentares, ou mesmo legais. A face mais facilmente visível disso é a obrigação imposta a qualquer organização que detenha dados cadastrais que possam ser vinculados a pessoas físicas, sejam internas ou externas à organização, estipulada pela Lei Geral de Proteção de Dados Pessoais, a LGPD (Lei 13.709/2018).

Entendido isso, fica patente que a organização deverá se equipar para a proteção de dados, e o compartilhamento de informações de cibersegurança aparece como componente de um dos "desenhos" possíveis dessa proteção. Dessa forma, é oportuno contextualizar essa atividade, do ponto de vista dos custos, dentro de um panorama que inclui as outras alternativas.

Uma organização possui um leque de opções para prover a proteção de seus dados sensíveis. Uma delas é a de manter uma estrutura própria, orgânica, responsável por todas as etapas de proteção, desde o inventário de ativos e dados, passando pelo levantamento de todas as vulnerabilidades e ameaças, a detecção e análise de quaisquer novas ameaças, o estabelecimento das medidas defensivas e sua implementação, até o acompanhamento da efetividade das ações de proteção.

Outra alternativa é a de contratar uma empresa terceira especializada, para zelar por todas essas atividades descritas, sem o envolvimento de capacidade própria, em uma situação de total dependência.

Uma outra rota de ação, que é a que nos interessa analisar em maior profundidade, é aquela em que a organização estabelece uma capacidade própria ou parcialmente terceirizada para essas atividades, incluindo a participação em uma Rede de Compartilhamento de Informações de Cibersegurança, pelas razões e métodos explorados nos capítulos anteriores.

Conforme o já exposto no capítulo dedicado ao modo de compartilhamento, existem recursos materiais e humanos que precisam ser empenhados para a efetiva participação da organização na rede de compartilhamento, e para o aproveitamento efetivo dos dados e informações dela obtidos, na internalização desses dados e informações para os dispositivos de proteção da organização.

Para o cálculo do custo financeiro de se manter a estrutura necessária para o compartilhamento das informações de cibersegurança, deve-se, seja por experiência ou por meio de estimativa por analogia, avaliar o volume, em homens-hora/mês, para a preparação de dados para o compartilhamento, e para a internalização de dados recebidos por compartilhamento. Considerando que a(s) pessoa(s) incumbida(s) dessas atividades utiliza(m) equipamento(s) institucional(is), deve-se computar o custo de uso/amortização desse(s) equipamento(s), em volume de horas alocadas à atividade. Dessa forma, o custo pode ser estimado/calculado em termos do valor de remuneração do(s) profissional(is) envolvido(s), considerando o padrão salarial dos colaboradores com o nível de instrução/formação necessários para as análises de segurança sofisticadas requeridas para o exercício da função, somado ao custo da "fatia" de tempo computacional necessário para "rodar" as atividades de preparação, recebimento e análise de dados compartilhados. Caso seja necessária a capacitação de um ou mais colaboradores para serem alocados nessa tarefa, isso precisa ser, necessariamente, provido.

Em casos específicos, em que se utilizem plataformas de compartilhamento proprietárias, que exigem o pagamento de licenças, e em que se participe de rede de compartilhamento que exija taxa de adesão e mensalidade de permanência, esses valores, iniciais e continuados, precisarão ser também computados, para se poder avaliar os valores que devem ser reservados exclusivamente para o emprego na atividade de compartilhamento de informações de cibersegurança.

Em resumo: Compartilhar dados custa o tempo de dedicação do colaborador remunerado, da sua formação, o tempo de uso de equipamento vis a vis sua amortização, e, eventualmente, licenças, joias e mensalidades.

Por fim: O modo como esses recursos serão providos inicialmente, e assegurados ao longo do tempo, dependerá do compromisso da organização com o cumprimento de suas obrigações legais e regulamentares em relação à proteção de dados.

Caso a organização, por sua visão de negócio, enxergue a Segurança da Informação como um investimento justificável, e não como um dispêndio obrigatório, terá oportunidades de ir além e acima do mero cumprimento de requisitos prescritivos, tornando a Segurança de Informação uma parte integrante e integral de seu conjunto de Sistemas de Gestão.

APÊNDICE - GUIA DE INSTALAÇÃO DO MISP

REQUISITOS DO SISTEMA

Antes de começar, certifique-se de ter os seguintes pré-requisitos:

- Sistema Operacional: Ubuntu 20.04/22.04 (recomendado), Debian, CentOS ou Red Hat.
- Memória: 4 GB (mínimo), 8 GB (recomendado).
- Armazenamento: Pelo menos 50 GB de espaço livre.
- Dependências:
    - » Apache2 ou Nginx (servidor web).
    - » MySQL/MariaDB (banco de dados).
    - » PHP 7.4+.
    - » Python 3.

PASSOS DE INSTALAÇÃO

Aqui estão os passos detalhados para a instalação do MISP:

1. Atualize o sistema

Primeiro, é importante garantir que seu sistema está atualizado.

```
sudo apt update && sudo apt upgrade -y
```

2. Instale os pacotes necessários

Instale os pacotes básicos, como Apache, MySQL e PHP, necessários para rodar o MISP:

```
sudo apt install apache2 mysql-server php libapache2-mod-php php-mysql php-redis php-pear php-zip php-bcmath php-mbstring php-xml php-gd redis-server python3 python3-dev python3-pip python3-venv git curl -y
```

3. Baixe o código do MISP

Crie um diretório para o MISP e baixe o código da plataforma a partir do repositório oficial:

```
sudo mkdir /var/www/MISP
cd /var/www/MISP
sudo git clone https://github.com/MISP/MISP.git /var/www/MISP
```

4. Configuração do Apache

Configure o Apache para servir o MISP. Crie um novo arquivo de configuração do Apache:

```
sudo nano /etc/apache2/sites-available/misp.conf
```

Insira as seguintes linhas:

```
<VirtualHost *:80>
    ServerAdmin admin@example.com
    ServerName misp.example.com
    DocumentRoot /var/www/MISP/app/webroot
    <Directory /var/www/MISP/app/webroot>
        Options -Indexes
        AllowOverride all
        Require all granted
    </Directory>
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Substitua `misp.example.com` pelo seu nome de domínio ou endereço IP.

Ative o site e reinicie o Apache:

```
sudo a2ensite misp
sudo systemctl reload apache2
```

5. Configuração do Banco de Dados

Acesse o MySQL e crie o banco de dados para o MISP:

```
sudo mysql -u root -p
No console do MySQL, execute os seguintes comandos:
CREATE DATABASE misp;
CREATE USER 'mispuser'@'localhost' IDENTIFIED BY 'senhaSegura';
GRANT ALL PRIVILEGES ON misp.* TO 'mispuser'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Substitua 'senhaSegura' por uma senha forte para o usuário do banco de dados.

6. Configuração do MISP

Copie o arquivo de configuração padrão do MISP:

```
cd /var/www/MISP/app/Config
sudo cp config.default.php config.php
```

Edite o arquivo de configuração para ajustar as variáveis do banco de dados:

```
sudo nano config.php
```

Busque pela seção de configurações do banco de dados e edite os valores conforme o seu setup:

```
'Datasources' => [
    'default' => [
        'host' => 'localhost',
        'login' => 'mispuser',
        'port' => '3306',
        'password' => 'senhaSegura',
        'database' => 'misp',
        'prefix' => '',
        'persistent' => false,
        'encoding' => 'utf8mb4',
    ],
],
```

Ajuste as permissões dos arquivos:

```
sudo chown -R www-data:www-data /var/www/MISP
sudo chmod -R 750 /var/www/MISP
sudo chmod -R g+ws /var/www/MISP/app/tmp
```

7. Configure o Python para os Enriquecimentos

Instale os requisitos Python e configure o ambiente virtual para o MISP:

```
cd /var/www/MISP/venv
python3 -m venv .
source bin/activate
pip install -r /var/www/MISP/requirements.txt
```

8. Inicialização do Redis e outros serviços

Habilite o Redis para rodar no boot e inicie o serviço:

```
sudo systemctl enable redis-server
sudo systemctl start redis-server
```

9. Finalização e Acesso

Agora, você pode acessar o MISP no navegador utilizando o IP ou nome de domínio do servidor:

```
http://misp.example.com
```

Use as credenciais padrão de admin para o primeiro login (geralmente 'admin@admin.test' e 'admin'), mas altere as senhas imediatamente.

CONFIGURAÇÕES ADICIONAIS

HTTPS: Para garantir a segurança, é altamente recomendável configurar SSL/TLS para acesso HTTPS. Use o Let's Encrypt para configurar SSL automaticamente:

```
sudo apt install certbot python3-certbot-apache
sudo certbot --apache
```

Atualização de Chaves GPG: MISP utiliza GPG para assinar objetos de confiança, então é importante configurar isso adequadamente.

REFERÊNCIAS

Centro de Inteligência de Segurança Cibernética (CISC). TLP - Traffic Light Protocol. CISC. Disponível em: https://www.gov.br/cisc/pt-br/tlp?formCode=MG0AV3. Acesso em: 26 de dezembro de 2024.

CERT.br. MISP - Malware Information Sharing Platform. CERT.br. Disponível em: https://www2.cert.br/misp/. Acesso em: 26 de dezembro de 2024.

Forum of Incident Response and Security Teams (FIRST). Traffic Light Protocol (TLP) Version 2.0. FIRST. Disponível em: https://www.first.org/tlp/docs/v2/tlp-pt-br.pdf. Acesso em: 26 de dezembro de 2024.

International Civil Aviation Organization (ICAO). Cyber Information Sharing. ICAO, Montreal. Disponível em: https://www.icao.int/aviationcybersecurity/Documents/Cyber%20Information%20Sharing.EN.pdf. Acesso em: 26 de dezembro de 2024.

Centro Integrado de Segurança Cibernética do Governo Digital (CISC). MISP (Malware Information Sharing Platform). Disponível em: https://www.gov.br/cisc/pt-br/etir-as-a-service/misp. Acesso em: 26 de dezembro de 2024.

MISP Project. MISP Features. MISP Project. Disponível em: https://www.misp-project.org/features/. Acesso em: 26 de dezembro de 2024.

ANAC AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL