Procedimento Operacional de Prevenção e Resposta a Incidentes de Segurança

Elaborado por: Marcelo Martinelli Marfil

Aprovado por: Rodrigo Strauss

Sumário

1. Objetivo

O objetivo do procedimento é estabelecer diretrizes para prevenir e garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos/serviços de informação ou recursos computacionais da INTELITRADER.

Entende-se por incidente de segurança toda ocorrência que possa vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da INTELITRADER.

Essas ocorrências devem ser tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados.

2. O que deve ser protegido:

Os seguintes componentes do sistema de informação da INTELITRADER devem ser protegidos e o plano de resposta a incidentes deve prever ação no caso de um incidente de segurança:

- Servidores:
  - Na Nuvem:
    - Oracle; Google; AWS; Azure; Contabo; DigitalOcean; Linode

- Bancos de dados:
  - RDS Amazon
    - Postgres
    - Mysql

  - Bancos de dados Sqlite nas instâncias do WTM e NTP

- Sistemas
  - Próprios
    - InteliMarket
    - InteliData
    - InteliMobile
    - InteliOrder
    - InteliRisk
    - Intelitrader Algorithm Plataform
    - WTM para WhatsApp
  - De terceiros
    - BitBucket
    - Jira
    - Jira Service Desk
    - Confluence
    - Backup

3. Incidentes:

Nesse procedimento vamos considerar ações para os seguintes incidentes:

- Roubo de credenciais
- Acesso não autorizado
- Denial of Service
- Distributed Denial of Service
- Contaminação por Malware
- Ransomware
- Exploração por vulnerabilidade de aplicação Web ou configuração do servidor HTTP
- Perda de dados

Roubo de Credenciais

O roubo de credenciais pode ocorrer de várias maneiras. O roubo pode acontecer de diversas formas:

- Ataque de força bruta.
- Repetição de senhas comprometidas em outros sistemas.
- Engenharia Social.
- Man in the Middle.

Acesso não autorizado

Acesso não autorizado pode ser realizado a partir de um roubo de senha, conforme explicado anteriormente, ou explorando alguma falha de segurança.
Dentre as consequências do uso indevido de credenciais citamos:

- Vazamento de informações sensíveis
- Tornar sistemas inoperantes
- Destruir ou alterar informações
- Acesso a outros sistemas

Denial of Service (DoS)

Denial of service é um ataque com objetivo de tornar inacessíveis serviços computacionais e dados. É provocada por uma sobrecarga na rede, no servidor ou na aplicação ou explorando uma falha que derrube o serviço ou servidor.

Distributed Denial of Service (DDoS)

Igual ao Denial of Service com a diferença que o ataque vem de múltiplas origens. A resposta a um DDoS é mais complexa e muitas vezes requer a colaboração do provedor de acesso à internet ou provedor de serviços na nuvem.

Contaminação por Malware

São vários os vetores de contaminação por malware. Os vetores de ataque de malware são:

- Engenharia Social: O principal vetor de transmissão de malwares. Consiste em induzir a vítima a fornecer informações confidenciais (credenciais de acesso, por exemplo) ou tomar ações como, por exemplo, instalar um malware ou acessar um site malicioso.

- Phishing: É uma forma de engenharia social que consiste no envio de emails ou mensagens (SMS, Skype, WhatsApp, etc) com links para sites maliciosos ou download de arquivos contaminados.

- Drive-by Downloads: Infecção causada pelo simples acesso a um site que explora vulnerabilidades no navegador. Não é necessária nenhuma ação para que a contaminação ocorra. Muitas vezes a página maliciosa foi comprometida sem o conhecimento do dono da página.

- Malware baseado em anúncio: Funciona da mesma forma que o Drive-by Downloads, mas o código malicioso é inserido em anúncios.

- Exploração pela rede de falhas de segurança de Sistemas Operacionais ou aplicações - malwares podem se espalhar na rede a partir de um computador comprometido na rede, mesmo sem nenhuma ação do usuário.

- Infecção de arquivos compartilhados na rede a partir de uma estação comprometida.

Ransomware
É um tipo de malware que criptografa os dados de um disco tornando-os inacessíveis. A chave para desbloqueio é fornecida após o pagamento de um “resgate”. Discos remotos (em servidores de arquivos ou NAS) podem ser atacados também.

Destacamos esse malware pela sua alta incidência e danos que podem causar.

Exploração de Vulnerabilidades
Falha numa aplicação Web ou mesmo na configuração do servidor HTTP pode ser explorada. Dependendo da falha, o atacante pode ter acesso a bancos de dados, a arquivos e páginas web e também executar comandos e instalar programas indesejados.

Perda de dados
Dados podem ser perdidos por problema de hardware ou até mesmo um apagamento involuntário. Medidas devem ser tomadas para restaurá-los.

4. Prevenção de Incidentes

A prevenção de incidentes é composta por uma série de ações e ferramentas visando a impedir incidentes de segurança.

As medidas de prevenção adotadas são:

- Uso de antivírus em estações e servidores;
- Uso de firewall de rede nos escritórios e na nuvem;
- Uso de criptografia em toda comunicação pela rede;
- Segmentação da rede onde necessário;
- Autenticação de acessos remotos;
- Backup dos dados;
- Testes periódicos de invasão;
- Criptografia de dados nos discos e banco de dados.

4.1 - Uso de antivírus

O uso de antivírus nas estações de trabalho e nos servidores protege contra a infecção por malware.

Deve possuir atualização automática para a prevenção de novas ameaças que surgem diariamente.

A infecção das estações de trabalho, além do roubo de dados armazenados no mesmo, também pode facilitar o acesso indevido a outros serviços e dados.

4.2 - Uso de firewall

Os servidores da Intelitrader são todos armazenados em nuvem e, desta forma, são protegidos por firewall que permite acesso apenas aos serviços necessários.

4.3 - Uso de criptografia

Toda a comunicação passando pela internet é criptografada.

Acessos remotos a servidores são feitos com SSH e acesso aos serviços Web usam o HTTPS.

Os acessos remotos aos servidores de clientes são feitos usando VPN IPSec.

4.4 - Segmentação de Redes

Os servidores hospedados na nuvem são agrupados em segmentos diferentes de rede conforme a sua aplicação e ambiente.

Os servidores de banco de dados só podem ser acessados dentro do mesmo segmento de rede, protegendo-os de ataques externos.

4.5 - Autenticação

Todos os acessos remotos aos servidores e banco de dados são autenticados por senha e/ou certificado digital.

4.6 - Backup

Todos os dados dos servidores e dos bancos de dados têm seus backups efetuados diariamente e os backups são armazenados conforme a seguinte política:

- Diário dos últimos 30 dias;
- Semanal das últimas 5 semanas;
- Mensal últimos 5 anos.

4.7 - Teste de invasão

Os fornecedores de armazenamento em nuvem são responsáveis pelos testes de invasão para detectar possíveis falhas de segurança que possam ser exploradas.

4.8 - Criptografia dos dados

Os dados armazenados no HD e nos bancos de dados serão criptografados para aumentar a confidencialidade dos dados.

5. Equipe de Resposta a Incidentes

Responsáveis:

Rodrigo Luis de Godoy Strauss Mello Vieira

e-mail: rodrigo.strauss@intelitrader.com.br

telefone: (11) 93960-0229

Marcelo Martinelli Marfil

e-mail: marcelo.marfil@intelitrader.com.br

telefone: (19) 99394-8751

6. Resposta a Incidentes

Diferentes tipos de incidentes requerem diferentes tipos de resposta que detalharemos a seguir. A resposta ao incidente inclui contenção da ameaça, restauração dos serviços e avaliação pós-incidente para melhoria da prevenção e, se necessário, eventual melhoria do plano de resposta.

Todos os incidentes e ações tomadas em resposta devem ser documentadas. Os seguintes dados devem ser registrados:

- Data e hora da detecção do incidente;
- Data e hora provável do início do incidente;
- Tipo de Incidente;
- Sistemas afetados;
- Dados comprometidos;
- Todas as ações tomadas, conforme o tipo de incidente;

- Conclusão com as causas do incidente e ações a serem tomadas.

7. Procedimentos Operacionais

7.1 Roubo de Credenciais

Dois tipos de credenciais podem ser usados, senha e certificados. Em ambos os casos as seguintes ações devem ser tomadas:

7.1.1 - Identificar todos os sistemas aos quais as credenciais possuem acesso
É necessário levantar todos os sistemas que podem ser acessados usando as credenciais roubadas.

7.1.2 - Alterar as senhas e certificados comprometidos
A partir do levantamento, alterar as senhas e certificados comprometidos.

7.1.3 - Tentar identificar a data e hora em que as credenciais foram comprometidas
Examinando os logs de acesso, tentar identificar o momento em que a credencial foi comprometida. Uma entrevista com o dono das credenciais também pode ajudar nesse processo.

7.1.4 - Analisar os acessos pela conta comprometida em todos os sistemas.
Se conseguirmos identificar a data e hora, a análise deve ser feita a partir desse momento. Caso contrário, a partir da 1ª semana antes da detecção do incidente.

7.1.5 - Restaurar sistemas afetados
Após a análise dos acessos, identificar-se-á o que foi comprometido nos sistemas. Por exemplo, verificar se foram instalados backdoors ou outro software malicioso.

Pode ser necessário restaurar o sistema a partir de imagens do sistema e backups

7.1.6 - Levantar dados comprometidos
Dados comprometidos são dados vazados e dados alterados ou apagados. No caso de dados alterados ou apagados, restaurar o último backup íntegro. No caso de dados vazados informar ao cliente.

7.1.7 - Reportar o incidente

Seguir o procedimento no item 7.5 deste Procedimento de Prevenção e Resposta a Incidentes de Segurança.

7.1.8 - Analisar como ocorreu o incidente e corrigir falhas
Identificar a falha de segurança que permitiu a violação das credenciais e corrigir o sistema de segurança para impedir novos incidentes.

7.1.9 - Avaliar o Plano de Resposta
Avaliar, a partir da experiência com o incidente, se há melhorias a serem feitas no plano de resposta a incidentes.

7.2 - Acesso não autorizado

Se o acesso não autorizado for a partir do roubo de credenciais, seguir com a troca das mesmas.

Outras formas de acesso não autorizadas podem acontecer e nesse caso deve ser seguido o plano a seguir.

Um acesso não autorizado sem roubo de credenciais pode ser conseguido explorando falhas de segurança no sistema operacional, serviços e aplicações.

7.2.1 - Analisar os acessos indevidos

Se conseguirmos identificar a data e hora, a análise deve ser feita a partir desse momento. Caso contrário, a partir da 1ª semana antes da detecção do incidente.

7.2.2 - Restaurar o sistema afetado

Após a análise dos acessos, identificar o que foi comprometido no sistema. Por exemplo, verificar se foram instalados backdoors ou outro software malicioso.

Pode ser necessário restaurar o sistema a partir de imagens do sistema e backups

7.2.3 - Levantar dados comprometidos

Dados comprometidos são dados vazados e dados alterados ou apagados.

No caso de dados alterados ou apagados, restaurar o último backup íntegro.

No caso de dados vazados informar ao cliente, se for o caso.

7.2.4 - Reportar o incidente

Seguir o procedimento no item 7.5 deste Procedimento de Prevenção e Resposta a Incidentes de Segurança.

7.2.5 - Analisar como ocorreu o incidente e corrigir falhas

Identificar a falha de segurança que permitiu a violação das credenciais e corrigir o sistema de segurança para impedir novos incidentes.

7.2.6 - Avaliar o Plano de Resposta

Avaliar, a partir da experiência com o incidente, se há melhorias a serem feitas no plano de resposta a incidentes.

7.3 - Denial of Service

Temos que diferenciar a resposta a um DoS de um DDoS. Se for um DDoS, seguir o plano em VI.4

7.3.1 - Identificar a origem do ataque

Verificando os logs identificar a origem do ataque

7.3.2 - Identificar o serviço atacado

Um ataque pode ser na rede, num serviço (ex: servidor Web). No caso de um ataque não distribuído, normalmente o ataque se dá num serviço.

7.3.3 - Bloquear ataque no Firewall
Bloquear o IP infrator no firewall.

7.3.4 - Restaurar o Serviço
Se o ataque derrubou o serviço, reiniciá-lo.

7.3.5 - Reportar o incidente
Contactar os clientes nos canais acordados relatando a falha e medidas já tomadas.

7.3.6 - Analisar como ocorreu o incidente e corrigir falhas
Identificar a possibilidade de melhorias na proteção contra ataques de DoS.

7.3.7 - Avaliar o Plano de Resposta
Avaliar, a partir da experiência com o incidente, se há melhorias a serem feitas no plano de resposta a incidentes.

7.4 - Distributed Denial of Service

7.4.1 - Identificar o ataque
Verificando os logs determinar portas e protocolo usados no ataque. Isso permite identificar o serviço atacado e a bloquear o ataque no firewall.

7.4.2 - Mitigar o efeito do ataque nos outros serviços
Se o ataque a um serviço estiver comprometendo outros serviços no servidor, considerar:

- Possibilidade de tirar o serviço do ar;
- Restringir o uso de recursos computacionais usados pelo serviço. No caso do servidor Web, o alvo mais provável, ajustar os seguintes parâmetros:
    - MaxClients/MaxRequestWorkers
    - MaxSpareThreads
    - MinSpareThreads

Se o serviço atacado for o único executado no servidor, esse passo é desnecessário.

7.4.3 - Conter ataque com o Firewall
Conter o ataque no firewall, limitando o número de acessos por minuto por IP. No iptables, usar uma regra como:

```
#iptables -A INPUT -p tcp --dport 443 --syn -m hashlimit
--hashlimit-mode srcip --hashlimit-upto 3/min --hashlimit-burst 2
--hashlimit-name conn_rate_limit -j ACCEPT


#iptables -A INPUT -p tcp --dport 443 --syn -j DROP
```

7.4.4 - Restaurar o Serviço
Após o ataque cessado:

- Voltar os parâmetros originais do serviço
- Reiniciar o serviço se necessário

7.4.5 - Reportar o incidente
Contactar os clientes nos canais acordados relatando a falha e medidas já tomadas.

7.4.6 - Analisar como ocorreu o incidente e corrigir falhas
Identificar a possibilidade de melhorias na proteção contra DDoS.

7.4.7 - Avaliar o Plano de Resposta
Avaliar, a partir da experiência com o incidente, se há melhorias a serem feitas no plano de resposta a incidentes.

7.5 Classificação dos Incidentes Quanto à Criticidade:

Um evento pode ser classificado de diversas formas de acordo com a sua severidade e comprometimento das operações e entregas de Service Level da empresa. Para este procedimento Operacional de Prevenção e Respostas a Incidentes de Segurança, determinamos os seguintes níveis de classificação de incidentes:

Crítica	Falha operacional completa, que afeta o negócio e o cliente.
Alta	Grave perda de capacidade operacional, que afeta o negócio e pode afetar o cliente.
Média	Impacto operacional substancial que pode afetar o negócio e o cliente.
Baixa	Impacto operacional perceptível, mas limitado pois não afeta o negocio e nem o cliente.

7.6 - Reportar o incidente

Todo o incidente de segurança da informação deve ser reportado diretamente aos gestores da Intelitrader e a equipe responsável pelo sistema afetado para imediato tratamento. Finalizado o incidente, o tema será tratado por todos os envolvidos em reunião dedicada.

Casos Classificados como críticos ou Alta Prioridade:

- Avisar ao cliente sobre a paralisação do serviço se exigido por contrato.
- Avaliar a necessidade de outras notificações conforme recomendação CERT.BR: https://www.cert.br/docs/whitepapers/notificacoes/#1

Casos Classificados como média ou Baixa Prioridade:

- Avaliar de acordo com o critério do Comitê Gestor da Segurança da Informação.

8. Registros

Identificação	Armazenamento	Proteção	Recuperação	Tempo de retenção	Forma de Descarte
Registro e respostas aos incidentes	Jira	Gestão de acesso	Por data Por assunto Por responsável	Indeterminado	N/A

9. Histórico de revisão

Data	Versão	Elaborado por	Descrição da alteração
05/11/2022	1	Fernanda Segatt	primeira edição
09/11/2022	2	Marcelo Marfil	revisão de correspondência de infra
10/11/2022	3	Rodrigo Strauss	revisão de termos e políticas

10. Anexos

Não aplicável