FAQ: Perguntas Frequentes ao CTIR Gov

Índice:

FAQ:

1- O que é o CTIR Gov?

É o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - APF. Está subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC - do Gabinete de Segurança Institucional da Presidência da República - GSIPR. Sua finalidade é o atendimento aos incidentes em redes de computadores da APF. Ademais, é um Centro de Coordenação com Responsabilidade Nacional, reconhecido pelo *CERT Coordination Center* (CERT/CC). No Brasil, o CTIR Gov e o CERT.br integram a lista de *National Computer Security Incident Response Teams* do CERT/CC. Saiba mais em Sobre o CTIR Gov..

2- Qual o papel do CTIR Gov?

O CTIR Gov atua como Equipe de Coordenação, fazendo a ligação entre os envolvidos e acompanhando as ações de tratamento e resposta aos incidentes. Para obter informações, tais como missão, histórico, legislação e estatísticas, acesse www.ctir.gov.br.

3- Quais os serviços prestados pelo CTIR Gov?

O conjunto de serviços providos pelo CTIR Gov à APF pode ser dividido em:

- Notificação de Incidentes;
- Análise de Incidentes;
- Suporte à Resposta a Incidentes;
- Coordenação na Resposta a Incidentes;
- Distribuição de Alertas, Recomendações e Estatísticas;

- Cooperação com outras Equipes de Tratamento de Incidentes.

Saiba mais em Sobre o CTIR Gov.

4- **O que é um incidente de segurança?**
A Norma Complementar nº 05/IN01/DSIC/GSIPR define Incidente de Segurança como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

5- **Quais tipos de incidentes são tratados pelo CTIR Gov?**
O Centro recebe notificações, no âmbito das redes da APF, de quaisquer eventos que sejam julgadas um incidente de segurança.
Esses incidentes podem ser varreduras (scans), tentativa de invasão, desfiguração de sítio, ataque de negação de serviço, ataque de engenharia social (phishing) e outros.

6- **Quem pode realizar notificações ao CTIR Gov?**

A comunicação entre os órgãos e instituições da APF e o CTIR Gov deve ocorrer, preferencialmente, por meio das Equipes de Tratamento de Incidentes em Redes Computacionais - ETIR ou por pessoas com esta atribuição.

7- **Como faço para entrar em contato com o CTIR Gov?**
Para notificação de incidentes de segurança o Centro atende por meio do correio eletrônico ctir@ctir.gov.br. As questões gerenciais ou relacionadas à Coordenação-Geral de Tratamento de Incidentes de Rede (CGTIR) podem ser tratadas por meio do e-mail cgtir@planalto.gov.br.

Para comunicação por meio de um canal seguro ou via INOC-DBA, acesse a página de Contato.

8- **Quais informações devo incluir em uma notificação de incidente?**
São dados essenciais a serem incluídos em uma notificação:

- Logs completos, com datas, horários e *timezones* dos registros;
- Dados completos do incidente, inclusive da sua respectiva detecção;
- Cabeçalhos completos do e-mail, no caso de *phishing*.

Leia na íntegra os Padrões para Notificação de Incidentes de Segurança de Rede ao CTIR Gov.

9- **O que acontece com as notificações enviadas ao CTIR Gov?**

Todas as mensagens encaminhadas ao Centro recebem tratamento adequado após o processo de triagem e análise. Via de regra, as ações desencadeadas pelas notificações têm como objetivo sanar os incidentes relatados e reestabelecer eventuais serviços comprometidos.

10- **O CTIR Gov realiza procedimentos de investigação judicial?**

Não. As atividades do Centro restringem-se à detecção, análise, resposta e tratamento de incidentes de rede. Eventuais desdobramentos judiciais devem ser procedidos por autoridade policial competente.

11- Por que devo notificar incidentes?

Ao ser notificado sobre um incidente de segurança, o CTIR Gov aciona as redes envolvidas com o intuito de mitigar ou cessar a atividade maliciosa. Além disso, o Centro contribui com a comunidade de segurança para a geração de assinaturas para a detecção de ataques.

Ademais, as informações recebidas são utilizadas para alimentar as bases de dados sobre incidentes, o que torna possível identificar tendências e padrões de atividades de invasores. A partir da análise desses dados, podem-se recomendar estratégias de prevenção adequadas para toda a comunidade da Administração Pública Federal, por meio da distribuição de alertas, recomendações e estatísticas.

Dessa forma, mesmo as redes que não foram envolvidas inicialmente em um incidente, podem ser beneficiadas pelo seu respectivo tratamento.

12- Qual a diferença entre Spam e Phishing?

Spam é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (*Unsolicited Commercial E-mail*).
Em função da elevada incidência de SPAM nas redes da APF e por oferecer menor risco em relação à segurança, **o CTIR Gov não trata Spam**.

Phishing, *phishing-scam* ou *phishing/scam*, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.
O *phishing* ocorre por meio do envio de mensagens eletrônicas que:

- Tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular;
- Procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- Informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
- Tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas Web.

*Definições obtidas na Cartilha de Segurança para Internet do Cert.br.

13- Como faço para notificar uma tentativa de fraude pela Internet?

A notificação deverá ser realizada por meio do correio eletrônico ctir@ctir.gov.br. A recomendação para as redes da APF que receberem e-mails de *phishing/scam* é que os enviem, com conteúdo e **cabeçalhos completos**.

14- Como o CTIR Gov atua nos casos de fraudes pela Internet?

As ações do Centro nos casos de fraudes pela Internet normalmente incluem:

- Neutralizar os canais de acesso a repositórios de códigos maliciosos, com o objetivo de mitigar o alcance da fraude, ainda que o usuário clique nos *links* utilizados na campanha de *phishing* do atacante;
- Contribuir para a ampliação da base de assinaturas dos antivírus e colaborar com a melhoria contínua dos sistemas de segurança, com o intuito de elevar a taxa de detecção das atividades maliciosas analisadas pelo CTIR Gov;
- Analisar o *malware*, verificar o seu comportamento e suas atividades, com vista a mitigar o alcance da fraude para os indivíduos que já tiveram seu computador comprometido;
- Distribuir alertas, recomendações e estatísticas, quando necessário.

15- Como o CTIR Gov realiza a detecção de incidentes?

A detecção de incidentes normalmente é realizada das seguintes formas:

Pelo próprio Centro por meio de seus sistemas de monitoramento e mecanismos de busca;

Por meio de notificação de terceiros, especialmente pelas ETIRs da APF e dos Estados, por outros CSIRTs nacionais ou internacionais, por colaboradores, por empresas de segurança, de instituições financeiras e outros.

16- Por que o CTIR Gov, em algumas notificações, inibe alguns dados como endereço IP, domínio e e-mail?

Em alguns casos o Centro substitui informações sensíveis por "xxx", "xxx.xxx.xxx.100", "xxx@xxx.gov.br", etc. O intuito é manter o sigilo de dados referentes a instituições, pessoas, computadores, sensores de detecção, etc.

Entretanto, essa sanitização não inviabiliza a identificação de registros em logs pois a substituição é parcial e outras informações são disponibilizadas para correlacionamento e filtro, como: data/hora, *timezone*, porta, protocolo, *flag*, URL, domínio e outros.

17- Quais as recomendações do CTIR Gov em caso de ocorrência ou suspeita de crime?

Em relação a esse aspecto, a Norma Complementar nº 08/IN01/DSIC/GSIPR estabelece:

"8.5 Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, as ETIR têm como dever, sem prejuízo do disposto no item 6 desta Norma Complementar e do item 10.6 da Norma Complementar nº 05/IN01/DSIC/GSIPR:
8.5.1 Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;
8.5.2 Observar os procedimentos para preservação das evidências exigindo

consulta às orientações sobre cadeia de custódia, conforme ato normativo específico a ser expedido;
8.5.3 Priorizar a continuidade dos serviços da ETIR e da missão institucional da organização, observando os procedimentos previstos no item 8.5.2."

18- O que é necessário para montar uma equipe de tratamento de incidentes de rede?

Os órgãos e entidades da APF devem adotar as instruções contidas na Norma Complementar nº 5, da Instrução Normativa nº 1/DSIC/GSIPR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR - nos órgãos e entidades da APF, direta e indireta.