Rating RCTS CERT

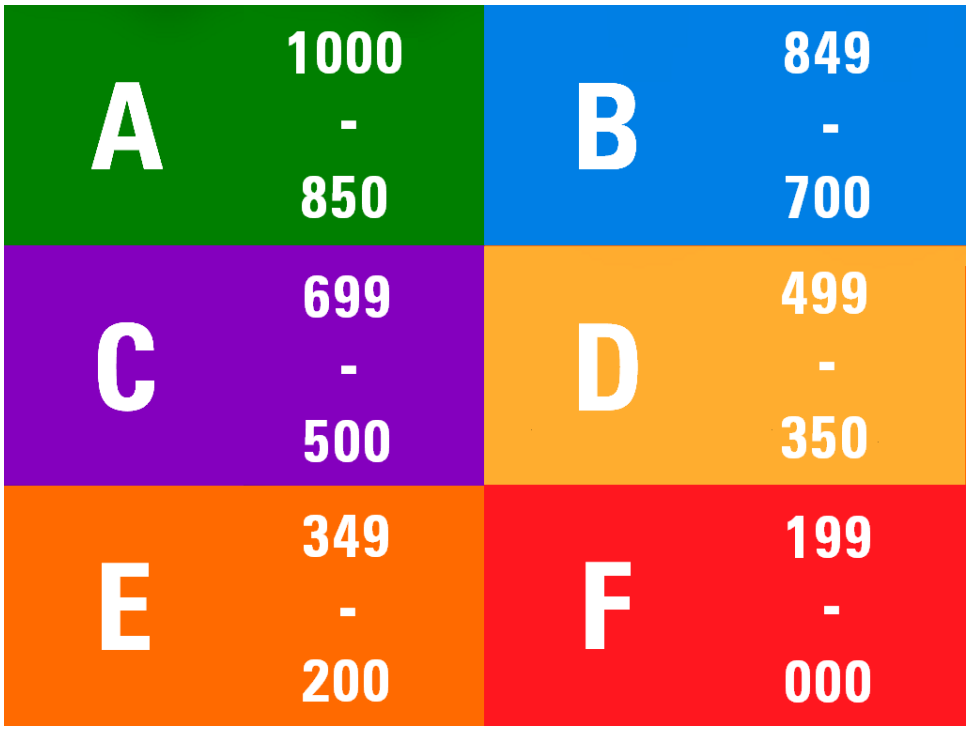
O Rating RCTS CERT é um score mensal composto actualmente por 16 parâmetros.

Sete desses parâmetros dependem de eventos, que podem variar de mês para mês, consoante dados recolhidos de diversas fontes. Os restantes nove parâmetros dependem de configurações ou no caso do último parâmetro, de cada organização decidir formalizar uma equipa de resposta a incidentes.

Sobre estes 16 parâmetros é construído um «score» que pode variar entre 0 e 1000.

Nenhum dos componentes tem um peso de menos de 5% e nenhum tem um peso de mais de 15%.

O «score» em cada mês dá origem a uma categoria, que varia de A (melhor) a F (pior), de acordo com os intervalos da figura abaixo:



As páginas seguintes deste documento detalham a lógica de cada parâmetro.

Qualquer dúvida deve ser dirigida a info@cert.rcts.pt

1) Incidentes

Este parâmetro incide sobre a actividade principal do RCTS CERT, que é a disponibilização de um ponto de contacto para que qualquer pessoa possa reportar um incidente que diga respeito à RCTS. O valor atribuído neste parâmetro depende do número de incidentes reportados (depois de efectuada a triagem pelo RCTS CERT) e dos dias em que as organizações demoram a fornecer feedback sobre a situação, que permita fechar os casos em aberto. Todos os incidentes são categorizados com base na Taxonomia da Rede Nacional CSIRT (https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf)

Fórmula de cálculo

Cada incidente desconta 1 ponto por cada dia em que permanecer aberto no sistema de registo de incidentes do RCTS CERT. Esta componente tem um peso de 15% no total do rating.

O que fazer?

Adquirir o máximo de conhecimento sobre a própria infraestrutura da organização e dispor de contactos agilizados com pessoas das diversas unidades orgânicas que gerem partes da infraestrutura e que possam intervir de forma efectiva em caso de incidente de segurança informática.

2) Malware

O RCTS CERT recebe eventos de malware de diversas fontes que consolida no seu SIEM. Apesar de as várias fontes não terem todas o mesmo grau de confiança, todos os eventos de malware são considerados da mesma forma.

Fórmula de cálculo

Cada evento de malware desconta 1 ponto. Esta componente tem um peso de 5% no total do rating.

O que fazer?

Os eventos de malware surgirão em maior quantidade em função do menor grau de protecção dos dispositivos que usam as infraestruturas de rede de uma organização. Realizar as actualizações de sistema operativo e de aplicações contribui para manter um bom estado dos dispositivos. Também é aconselhável descontinuar todos os sistemas que deixem de ser necessários ou que fiquem sem um responsável pela sua gestão.

3) Direitos de Autor (Queixas sobre)

Com alguma frequência o RCTS CERT recebe queixas relativas a violações de direitos de autor (copyright). Essas queixas identificam sempre um endereço IP associável a uma organização. Estes eventos indiciam que existem utilizadores (voluntariamente) ou sistemas infectados a usar recursos da organização que estão a violar a lei.

Fórmula de cálculo

Cada queixa recebida desconta 5 pontos. Esta componente tem um peso de 5% no total do rating.

O que fazer?

Implantar mecanismos de detecção de utilização de protocolos peer-to-peer, que são habitualmente usados neste tipo de violação da lei.

Sensibilizar internamente os utilizadores das infraestruturas da organização de que os recursos disponibilizados não podem servir para violar a lei.

4) Defacements

«Defacement» é um tipo de ataque no qual um atacante consegue alterar o conteúdo e a aparência visual da homepage, de uma página particular, ou até mesmo de todo um domínio web, e assim substituir o conteúdo exibido no website com o seu próprio conteúdo. O defacement pode estar associado a outros tipos de ataques como SQL Injection, Cross-Site Scripting (XSS), DNS hijacking, infecções por malware, e acesso não autorizado. Através das diversas fontes que o RCTS CERT usa, podemos receber também informação de que um domínio foi blacklisted por motivo de defacement.

Fórmula de cálculo

Cada «defacement» desconta 10 pontos. Esta componente tem um peso de 5% no total do rating.

O que fazer?

A não ocorrência de «defacements» depende essencialmente de os sistemas expostos à Internet estarem devidamente protegidos e actualizados. Websites não geridos são habitualmente um problema. As auditorias periódicas poderão contribuir para encontrar vulnerabilidades, que, ficando latentes representam um risco acrescido.

5) IDS (Intrusion Detection System)

Esta componente está ligada à manutenção dos sistemas e dispositivos livres de malware. No caso de algum sistema comprometido atacar as redes da FCCN, os sistemas de detecção de intrusões existentes identificarão a proveniência desses ataques. De referir que a aplicação desta componente é extremamente limitada, pois só leva em conta casos onde a infraestrutura da FCCN é atacada/abusada.

Fórmula de cálculo

Cada detecção desconta 10 pontos. Esta componente tem um peso de 5% no total do rating.

O que fazer?

Minimizar as intrusões e os sistemas internos comprometidos que possam vir a atacar a infraestrutura da FCCN ou outras. No caso de serem detectados sistemas comprometidos deve-se bloquear o seu acesso à internet, em primeira instância, analisá-los se o dispositivo for da organização e por último reinstalá-los ou recomendar a sua reinstalação se se tratarem de dispositivos que são propriedade de terceiros.

6) Blacklists

A presença de endereços IP de uma instituição em blacklists pode afectar o bom funcionamento de diversos serviços ou aplicações. Este vector deve também ser entendido como um dano reputacional da organização. Os casos mais comuns de inclusão em blacklists resultam na impossibilidade de receber ou enviar mensagens de correio electrónico relativamente a determinados domínios.

Fórmula de cálculo

Cada inclusão em blacklists desconta 5 pontos. Esta componente tem um peso de 10% no total do rating.

O que fazer?

Manter a vigilância, para imediatamente reportar que o problema foi solucionado e que os endereços ou domínios da organização devem ser removidos das blacklists onde passaram a estar, minimizando desta forma qualquer impacto em serviços ou aplicações. Nem todas as blacklists permitem um «de-list» imediato, e em caso de reincidências torna-se também mais difícil solicitar as remoções.

7) Vulnerabilidades

As vulnerabilidades estão normalmente associadas a serviços expostos na Internet que podem ser abusados, e dar origem a incidentes.

Fórmula de cálculo

Cada vulnerabilidade encontrada desconta 2 pontos. Esta componente tem um peso de 10% no total do rating.

O que fazer?

As vulnerabilidades são cada vez mais importantes, permitindo a actores maliciosos comprometer sistemas vulneráveis. É importante aplicar as actualizações que são publicadas, nomeadamente as que dizem respeito ao sistema operativo.

8) E-MAIL - SPF

SPF é um registo DNS (do tipo TXT) que lista todos os servidores autorizados a enviar emails a partir de um certo domínio. Um servidor ao receber um email vai verificar os registos SPF desse domínio e verifica se o IP do servidor que enviou o email se encontra nessas lista de IPs autorizados.

Fórmula de cálculo

A existência de registo Sender Policy Framework (SPF) vale 50 pontos. Esta componente tem um peso de 5% no total do rating.

O que fazer?

É necessário criar um registo SPF adicionado à zona DNS de cada domínio. Aqui devem estar especificados que endereços IP ou hostnames é que estão autorizados a enviar emails deste domínio.

https://support.google.com/a/answer/10685031?hl=en

9) E-MAIL - DMARC

DMARC é um protocolo para autenticação de emails. Permite verificar se o email é legitimamente de quem o enviou, e o que fazer se não for.

DMARC permite indicar que as mensagens enviadas estão protegidas com SPF e DKIM, e indica como processar o email caso essas verificações falhem.

Fórmula de cálculo

Esta componente vale 50 pontos se existir um registo DMARC associado ao domínio principal da instituição, o que tem um peso de 5% no total do rating.

O que fazer?

É necessário existir um registo SPF adicionado à zona DNS do domínio. Estes validam a origem dos emails através da comparação do IP do endereço de email, contra o IP do dono do domínio que o envia.

Exemplo de um registo DMARC TXT da Microsoft:

_dmarc.microsoft.com. 3600 IN TXT "v=DMARC1; p=none; pct=100; rua=mailto:d@rua.contoso.com; ruf=mailto:d@ruf.contoso.com; fo=1"

Mais informações de configuração em:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide

https://mxtoolbox.com/dmarc/dmarc-setup?lm=NAV-PD

10) E-MAIL - DKIM

DKIM é um tecnica de autenticação de email que ajuda a prevenir que agentes maliciosos se façam passar por domínios legítimos.

Tem dois aspetos principais, o registo DKIM guardado no DNS e o header DKIM adicionado a todos os emails do domínio.

DKIM usa criptografia de chave pública para autenticar de onde vem o email e qual o agente que o envia. A chave privada é utilizada para assinar as mensagens e a chave pública, guardada no registo DKIM, é usada para verificar a assinatura.

Fórmula de cálculo

Esta componente vale 50 pontos se o DKIM estiver configurado no principal domínio da instituição. Representa 5% do valor global do rating.

O que fazer?

Em primeiro lugar é necessário gerar um par de chaves.

De seguida temos de colocar a chave pública gerada como um registo TXT nos settings do DNS. Cada DNS provider pode ter uma forma diferente de configurar isto, pelo que é recomendada uma investigação para cada caso.

Por fim é preciso um milter (email filter) que permita adicionar um header ao email com a chave privada gerada anteriormente.

Mais informações de configuração em:

https://www.mailjet.com/blog/deliverability/setting-up-dkim-step-by-step/

11) Web - Headers

A ideia principal para o uso de headers é melhorar a navegação e experiência do cliente. Melhora a cibersegurança pois permite-nos evitar o seu uso por atacantes em alguns vetores de ataque e deve por isso ser tido em consideração nas configurações do website principal da instituição.

Fórmula de cálculo

A existência de todos os headers corresponde a 50 pontos, e representa 5% do valor total.
Entre 3 e 4 headers corresponde a 25 pontos.
2 ou menos headers encontrados corresponde a 0 pontos.

Neste momento a nossa verificação assenta sobre a existência de alguns headers, em particular verificamos se existem os seguintes cinco headers:

- Strict-Transport-Security
- X-Frame-Options
- X-XSS-Protection
- Content-Security-Policy
- X-Permitted-Cross-Domain-Policies

Neste momento são testados 5 headers, mas no futuro esta lista pode ser aumentada ou reduzida o que implicará uma revisão da fórmula de cálculo.

O que fazer?

Para obter a pontuação máxima nesta compontente todos os cinco headers referidos acima devem existir. Estes headers, por regra, são activados ou inibidos na configuração do próprio servidor web.

12) Web-Server Signature

Nesta verificação o que fazemos é garantir que nenhum dos headers usados tem versões que possam ser usadas para identificar vulnerabilidades, e posteriormente identificar alvos de possiveis ataques.

Fórmula de cálculo

Esta verificação representa 5% do valor total ou 50 pontos. Por cada header com possiveis indicadores de versões são descontados 25 pontos ao valor total da verificação.

No imediato estamos a testar 2 dos headers mais conhecidos por conterem essa informação:

- server
- x-powered-by

O que fazer?

Devem ser removidos da configuração do servidor web quaisquer headers que contenham versões específicas.

13) DNS do domínio principal – Zone Transfer

A transferência de zona de um domínio DNS é algo que deve estar sempre limitada, uma vez que estando publicamente disponível representará um valioso contributo para qualquer acção de reconhecimento que mais tarde vise o ataque a uma instituição.

Fórmula de cálculo

Se a transferência de zona do domínio principal da instituição estiver inibida serão atribuídos 50 pontos (5% do valor do rating). Se a transferência de zona for permitida serão atribuídos 0 pontos.

O que fazer?

Na configuração de todos os servidores DNS autoritativos para o seu domínio deve estar inibida a transferência de zona. A transferência de zona só deve ser permitida no servidor primário (SOA – Start of Authority) para o servidores secundários (listados nos registos NS do próprio domínio).

14) DNS do domínio principal - DNSSEC

A configuração de DNSSEC permite aumentar o grau de segurança do DNS. A existência de DNSSEC configurado inibe alguns tipos de ataques como *cache poisoning* e *answer forgery*.

Fórmula de cálculo

A existência de DNSSEC configurado no principal domínio da instituição vale 50 pontos (ou seja 5% do valor total do rating).

O que fazer?

A plataforma webcheck.pt pode ser usada para verificar se o DNSSEC está configurado num determinado domínio.

Em https://www.pt.pt/pt/seguranca/dnssec/ estão várias referências que serão úteis para configurar DNSSEC no seu domínio.

15) Web - SSL

Actualmente é importantíssimo usar certificados SSL para garantir aos utilizadores dos websites que estão a visitar o website que pretendem, e que não estão a ser vítimas de algum processo fraudulento. Esta componente tem a especificidade de a qualidade do certificado SSL poder assumir diversos graus.

Fórmula de cálculo

Esta componente vale 50 pontos, representando 5% do valor global do rating. Se a qualidade do certificado for acima de "B" ou superior serão atribuídos os 50 pontos, se for entre "C" e "D" serão atribuídos 20 pontos. No caso de o certificado existir, mas por alguma razão não ser inteiramente confiável serão atribuídos apenas 5 pontos. O valor será de 0 pontos se o certificado SSL não existir.

O que fazer?

Caso ainda não tenha certificado SSL ou deseje melhorar a sua qualidade, deverá solicitar o seu certificado SSL ao serviço RCTS Certificados (https://www.fccn.pt/seguranca/rcts-certificados). Após a devida obtenção e instalação poderá testar a qualidade do certificado já instalado recorrendo ao teste da SSLLabs: https://www.ssllabs.com/ssltest.

16) Equipa CSIRT formalizada

A formalização de uma equipa de resposta a incidentes contribui para a cibersegurança global de qualquer organização. Uma equipa CSIRT é um conjunto de recursos humanos, ferramentas, processos e questões organizacionais. Não é necessário que existam recursos humanos dedicados, mas no limite é necessário que estejam identificadas as pessoas que no dia-a-dia vão colaborar para responder aos incidentes de segurança informática que possam surgir.

Fórmula de cálculo

A existência de equipa formalizada vale 50 pontos. Esta componente tem um peso de 5% no total do rating.

O que fazer?

Preencher um template de RFC2350 e disponibilizá-lo publicamente numa página web.

Notificar o RCTS CERT da formalização da equipa, para que possa ser adicionada ao índice de equipas em https://cert.rcts.pt/pt/rede-academica-de-csirts, onde se encontram também referências para diversos exemplos de RFC2350 preenchidos pelas várias equipas já existentes.