Organização Pan-Americana da Saúde
Organização Mundial da Saúde
ESCRITÓRIO REGIONAL PARA AS Américas

162ª SESSÃO DO COMITÊ EXECUTIVO

Washington, D.C., EUA, 18 a 22 de junho de 2018

Tema 7.4 da agenda provisória

CE162/INF/4
11 de abril de 2018
Original: inglês

CIBERSEGURANÇA NA OPAS

Introdução

1. Como as ameaças cibernéticas continuam repercutindo nas organizações internacionais, a Repartição Sanitária Pan-Americana (RSPA) está comprometida com o fortalecimento das medidas de cibersegurança necessárias para proteger dados e manter um ambiente digital seguro.

2. Este documento informa sobre os esforços da RSPA para avaliar e fortalecer a cibersegurança. Proporciona um resumo das iniciativas em curso e do roteiro elaborado para fortalecer ainda mais a postura da Repartição em relação à cibersegurança.

Antecedentes

3. A RSPA utiliza extensivamente a tecnologia da informação (TI) para realizar seu trabalho. Tendo em vista este aumento na dependência da tecnologia, faz-se imperativo mister manter continuamente um alto nível de confiança na segurança dos dados da RSPA.

4. Em 2016, a RSPA recebeu assessoria estratégica em cibersegurança do Centro Internacional de Computação das Nações Unidas (UNICC, por sua sigla em inglês). As medidas de cibersegurança existentes foram comparadas às boas práticas da indústria delineadas pela Organização Internacional para Padronização (ISO, por sua sigla em inglês) na norma ISO 27001, e um Roteiro de Cibersegurança foi elaborado.

Conquistas no ano de 2017

Conclusão da avaliação de conformidade à ISO 27001

5. Em 2017, a RSPA concluiu uma avaliação de cibersegurança que comparou os controles atualmente implementados às boas práticas da indústria, conforme delineadas na norma ISO 27001. A ISO 27001, parte da série ISO 27000, é uma norma amplamente aceita que identifica os requisitos para estabelecer, implementar, operar, monitorar, analisar, manter e melhorar continuamente um sistema de gestão da segurança da informação. Como

parte deste avaliação se examinou a conformidade à norma no contexto da missão da Organização Pan-Americana da Saúde (OPAS).

6. A avaliação utilizou o Modelo de Maturidade da Capacidade para medir a maturidade dos controles de segurança da informação já implementados pela RSPA. Durante o curso da avaliação, vários pontos fortes nas capacidades da cibersegurança da RSPA foram identificados, inclusive:

a) criação de um cargo de responsável pela segurança da informação em tempo integral;

b) assessoramento contínuo em matéria de segurança da informação estratégicas, fornecida pelo UNICC;

c) esforços contínuos para implementar serviços de segurança gerenciados externamente para segurança de rede;

d) marco consolidado para políticas e procedimentos de segurança da informação;

e) capacidade de backup e recuperação de dados;

f) uso de sistemas de proteção contra programas maliciosos (*antimalware*) em toda a Organização;

g) uso de programas para detectar vulnerabilidades em toda a Organização;

h) resposta a incidentes de segurança informática integrada ao Plano de Continuidade de Negócios;

i) modernização dos *firewalls* e *web filtering* em toda a Organização;

j) aprimoramento da segurança da infraestrutura de redes sem fio;

k) fortalecimento dos controles de acesso físico aos centros de dados da RSPA;

l) requisitos contratuais de cibersegurança integrados aos contratos dos fornecedores.

7. A avaliação classificou as recomendações como sendo de alta, média ou baixa prioridade, dependendo da harmonização com os requisitos da norma ISO. Ao todo, houve duas recomendações de alta prioridade, quatro recomendações de média prioridade e nove recomendações de baixa prioridade.

8. As duas recomendações de alta prioridade conclamaram a RSPA a fortalecer sua capacidade de resposta a incidentes de segurança informática e aumentar a conscientização sobre cibersegurança na força de trabalho da Organização. O estudo também recomendou aumentar as capacidades operacionais de cibersegurança para detectar e remediar pontos fracos e ameaças no ambiente existente de TI.

Finalização da avaliação da segurança do PMIS

9. Uma avaliação da segurança do Sistema de Informação para a Gestão da RSPA (PMIS, por sua sigla em inglês) também foi realizada. A avaliação consistiu em comparar

os controles implementados no ambiente do PMIS àqueles recomendados *a)* pela norma ISO 27001 sobre sistemas de gestão da segurança da informação, e *b)* pela Cloud Security Alliance. A Cloud Security Alliance promove o uso de boas práticas para fornecer garantias de segurança na computação em nuvem, e oferece capacitação sobre os usos da computação em nuvem para ajudar a manter seguras todas as outras formas de computação. A avaliação não identificou vulnerabilidades críticas à segurança da informação. Foram identificadas nove recomendações de prioridade média para melhorar ainda mais a cibersegurança da plataforma.

Incidentes de cibersegurança

10. Durante 2017, a RSPA não registrou nenhum incidente de cibersegurança crítico que afetasse o sigilo, a disponibilidade ou a integridade das informações da RSPA ou seus recursos de TI. A RSPA sofreu vários incidentes de phishing em 2017, com a finalidade de adquirir nomes e senhas de usuários para realizar atividades não autorizadas em sistemas da RSPA. Com as suas atuais capacidades da cibersegurança, a RSPA conseguiu detectar esses incidentes e executar controles de mitigação, e não detectou qualquer atividade não autorizada em seus sistemas de TI. A RSPA também observou que as capacidades de cibersegurança do provedor do PMIS desempenharam uma função crucial ao prevenir qualquer transação não autorizada. O aumento da frequência e complexidade dos incidentes de phishing, porém, indicou uma necessidade de reforçar os mecanismos de controle de acesso à informação dos sistemas de TI da RSPA, e esta recomendação foi incluída no Roteiro de Cibersegurança detalhado a seguir.

Roteiro de cibersegurança

11. Com base nas recomendações das avaliações e nos incidentes de segurança detectados, e de acordo com o plano estratégico da Organização, a RSPA elaborou um Roteiro de Cibersegurança que identifica projetos e iniciativas para melhorar a cibersegurança. Vários daqueles identificados no guia foram implementados em 2017, e outros serão implementados ao longo de 2018 e 2019. A implementação dessas iniciativas aprimorará a maturidade das capacidades da cibersegurança da RSPA e melhorará a capacidade da Repartição de proteger sua informação.

12. Os seguintes projetos e iniciativas foram realizados em 2017 para melhorar as capacidades de cibersegurança da RSPA, conforme o Roteiro de Cibersegurança:

a) *Recrutamento de um responsável pela segurança da informação em tempo integral:* O recrutamento do responsável pela segurança da informação foi concluído em 2017.

b) *Notificação e monitoramento por antivírus:* A proteção de antivírus em uso passou por upgrade para versão mais recente de modo a melhorar as capacidades de vigiar e detectar ameaças avançadas. Além disso, foram implementadas capacidades de alerta que fortalecem a capacidade da Organização para responder a incidentes graves com vírus.

c) *Consolidação e implementação de firewalls e serviços gerenciados de segurança:* A RSPA concluiu a implementação de serviços externamente gerenciados de segurança em 28 locais para proteger a infraestrutura de TI da Organização das ameaças externas. Nos dois locais restantes, os esforços serão concluídos no primeiro trimestre de 2018.

d) *Serviços de inteligência para detecção de ameaças:* Foi feita a assinatura de um serviço externo de inteligência com a intenção de receber precocemente notificações sobre ciberameaças que poderiam afetar a RSPA. O serviço permitirá à RSPA receber relatórios de inteligência sobre agentes e redes que representan ameaças e estão involvidos em crimes cibernéticos, *hacking* e fraudes, aproveitando o seu acesso único às comunidades de agentes maliciosos na *dark web* e na *deep web*. As informações relevantes serão triadas e encaminhadas à RSPA. Esta assinatura também proporcionará à RSPA o acesso a informações de inteligência de outras agências das Nações Unidas que assinam o serviço. Além disso, o serviço permitirá a RSPA monitorar a *dark web* para possíveis roubos de credenciais.

e) *Serviço de classificação de riscos de segurança:* Um serviço de classificação de riscos de segurança monitora a presença da Organização na Internet e gera alertas quando uma vulnerabilidade ou incidente de segurança é observado. Esta assinatura também proporciona à RSPA uma classificação de segurança que indica a eficácia das capacidades da cibersegurança da RSPA e permite à RSPA comparar seu programa de cibersegurança com aqueles de outras agências das Nações Unidas. Qualquer aumento ou queda da classificação de segurança gera um alerta que será monitorado.

f) *Reuniões regulares para discussão de segurança com todas as Representações da RSPA nos Países e com os Centros Pan-Americanos:* Foram implementadas reuniões mensais ordinárias com todas as Representações e Centros, com o objetivo de discutir o progresso na implementação do Roteiro de Cibersegurança.

g) *Teste de penetração:* Foi realizado um teste da segurança de uma aplicação crítica. O objetivo era avaliar as medidas de cibersegurança implementadas para proteger a informação armazenada e processada pela aplicação. O teste não identificou nenhuma vulnerabilidade crítica.

h) *Aperfeiçoamento do sistema de gestão de vulnerabilidades:* O software de monitoramento de vulnerabilidades já utilizado foi aperfeiçoado e configurado de modo a obter um diagnóstico global das vulnerabilidades que afetam os sistemas de TI da RSPA. Essa ferramenta desempenhou uma função crucial ao proteger os sistemas de TI da RSPA contra o incidente global conhecido como "*WannaCry*", que ocorreu no segundo trimestre de 2017. O WannaCry atingiu supostamente milhares de computadores em mais de 150 países em escala mundial, mas os sistemas de TI da RSPA não foram afetados e permaneceram protegidos através do monitoramento contínuo fornecido por este software.

i) *Proteção contra ameaças avançadas:* A proteção contra ameaças avançadas da Microsoft foi adquirida com o intuito de melhorar a capacidade de detectar e

responder a ciberameaças. A implementação deste sistema fornecerá proteção preventiva, permitirá detecção de ciberataques e permitirá administração centralizada ao longo de todo o ciclo de vida de segurança dos sistemas de TI da RSPA.

j) *Desativação de sistemas obsoletos:* Aproximadamente 63 sistemas obsoletos foram desativados com o intuito de reduzir vulnerabilidades que não estavam sendo remediadas através de patches pelos fornecedores.

k) *Consolidação e aperfeiçoamento da gestão de patches de segurança:* O programa usado para instalar patches de segurança nos computadores foi consolidado mais ainda para assegurar que possa ser monitorado de maneira centralizada.

l) *Proteção do website público da OPAS:* Um *firewall web* foi instalado para proteger ainda mais o website público da OPAS contra ciberataques. Este serviço protegerá contra ameaças avançadas persistentes que visam o website público da OPAS. Além disso, o serviço melhorará o desempenho e a entrega do website.

m) *Conscientização sobre segurança:* Vários boletins sobre segurança de informação foram circulados na RSPA para criar conscientização entre os usuários sobre ciberameaças como phishing, ransomware e vírus, e também para fornecer informações gerais sobre cibersegurança.

13. Vários projetos de cibersegurança devem ser finalizados em 2018-2019. Os parágrafos abaixo resumem brevemente esses projetos, por categoria:

a) *Aperfeiçoamento dos mecanismos de autenticação e controle de acesso digital:* Esses projetos visam melhorar ainda mais os mecanismos empregados pela RSPA para proteger os serviços como o PMIS, correio eletrônico e acesso remoto. Esses projetos também protegerão os sistemas de TI da RSPA das ciberameaças mais prevalentes na atualidade, que têm como alvo vulnerabilidades nos mecanismos de autenticação e controle de acesso.

b) *Melhoramento das capacidades de resposta a ciberincidentes:* Como é impossível prevenir totalmente a ocorrência de ciberincidentes, os projetos desta categoria visam fortalecer as capacidades de resposta e remediação de ciberincidentes pela RSPA.

c) *Conscientização sobre segurança da informação:* A RSPA continuará implementando o seu programa de conscientização sobre segurança da informação para incluir diferentes maneiras de aumentar a conscientização dos usuários que têm acesso aos recursos de informação da RSPA.

d) *Proteção dos sistemas de informação da RSPA publicamente acessíveis:* A RSPA continuará implementando vários projetos que visam aumentar as defesas que protegem os seus sistemas de informação publicamente acessíveis de serem visados por agressores com o intuito de comprometer a cibersegurança dos sistemas de informação da RSPA.

e) *Aperfeiçoamento das capacidades de monitoramento e alerta:* Com a complexidade e frequência cada vez maiores de ciberameaças, a RSPA aumentará e melhorará as capacidades de monitoramento de segurança que visam à detecção rápida de ciberincidentes. Essas iniciativas melhorarão significativamente as técnicas de resposta e remediação já em vigor na RSPA, e permitirão à RSPA realizar detecção precoce e remediação de vulnerabilidades informáticas.

14. A implementação das diversas iniciativas identificadas no Roteiro de Cibersegurança melhorará a postura da RSPA em relação à cibersegurança para alinhá-la ainda mais com as recomendações da ISO 27001. Essas iniciativas estão de acordo com as boas práticas da indústria e melhorarão as capacidades da RSPA de detectar, reagir e remediar incidentes da cibersegurança, além de aprender com eles.

Ação pelo Comitê Executivo

15. Solicita-se que o Comitê Executivo tome nota deste relatório e ofereça as observações que considere pertinentes.

- - -