BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

MAIO 2021 | nº 2/2021

DESTAQUES

Vulnerabilidades

No início de 2021 foi descoberto um conjunto de vulnerabilidades no Microsoft Exchange (uma aplicação que fornece serviço de *email*) que permitem o acesso indevido de agentes maliciosos aos sistemas e aos *emails* dos clientes deste serviço, entre outras ameaças, colocando em risco muitas organizações no mundo.

Atuação

Estas vulnerabilidades possibilitam a realização de intrusões, por exemplo, através da instalação de uma chamada "Web Shell" (DART, 2021), que facultam o acesso ao servidor e o acionar de um controlo remoto, conduzindo ao furto de dados ou à instalação de *malware*, nomeadamente *ransomware*. Julga-se que estas vulnerabilidades existiam há cerca de 10 anos, embora se pense que a sua exploração efetiva seja recente (Krebs, 2021).

Impacto

Este tipo de ação tem um grande potencial de impacto, tendo sido verificadas a nível internacional atividades de exploração destas vulnerabilidades por parte de grupos ligados a Estados, que procuram realizar ações de ciberespionagem, e grupos cibercriminosos, que pretendem ganhos financeiros. Em Portugal, o CNCS acompanha a situação através da análise das vulnerabilidades nos sistemas e do contacto com entidades potencialmente afetadas (DTIT, 2021).

VISUALIZAÇÃO

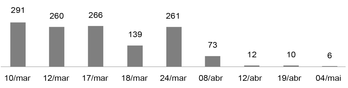
Entre o dia 10 de março e o dia 4 de maio de 2021 o CERT.PT:

- Contactou 84 entidades com servidores Microsoft Exchange vulneráveis, das seguintes áreas: Administração Pública Central, Regional e Local; Agricultura; Comunicação Social; Cultura; Defesa; Distribuição de Água Potável; Ensino Superior; Prestadores de Serviços de Internet/Telecomunicações; Prestadores de Serviços Digitais; além de organizações ligadas à Indústria;
- Identificou 1318 servidores Microsoft Exchange vulneráveis, verificando-se que 1254 viram corrigidas as referidas vulnerabilidades, até ao dia 4 de maio (este processo de contacto prossegue).

Estas entidades foram contactadas pelo CERT.PT em vários momentos no sentido de realizarem as medidas de mitigação necessárias, sobretudo as atualizações ao sistema. Foi ainda enviado um alerta com vista a reforçar junto da comunidade a informação técnica sobre estas vulnerabilidades e as boas práticas de prevenção e reação.

Entidades contactadas	84
Total de servidores identificados	1318
Vulnerabilidades corrigidas	1254
Vulnerabilidades por corrigir (até 4 de maio)	64

Nº de IPs vulneráveis (não repetidos) reportados pelo CERT.PT a entidades, entre 10 de março e 4 de maio de 2021



(Fonte: CERT.PT)

PERSPETIVA

1 As tecnologias digitais são desenvolvidas com um grande nível de complexidade e em prazos cada vez mais curtos, o que resulta na persistência de vulnerabilidades de segurança que podem demorar anos até serem descobertas. Se forem identificadas por algum agente de ameaças no ciberespaço, podem ser exploradas de modo discreto com o fim de se realizar intrusões em sistemas, instalar *malware* ou furtar dados, entre outros tipos de ameaças.

2 O mundo físico também apresenta vulnerabilidades de segurança. Por exemplo, uma fechadura com defeito coloca em causa o nível de segurança de um cofre. Contudo, as vulnerabilidades de segurança no contexto do mundo físico são colocadas à prova de modo menos sistemático e não permitem a exploração por parte de qualquer indivíduo que se ligue à Internet em qualquer lugar do mundo.

3 Este nível de exposição obrigou à criação de um sistema de padronização de identificação destas vulnerabilidades, o chamado "Common Vulnerabilities and Exposures" (CVE), o qual identifica cada vulnerabilidade através de um código e de um descritivo que permite uma compreensão objetiva das características da vulnerabilidade em causa. Este sistema foi criado em 1999 e desde então tem sido adotado pela comunidade e pelas instituições da área da cibersegurança.

4 A vitalidade do sistema CVE resulta do espírito de comunidade que a cibersegurança exige, funcionando com os contributos de profissionais ou interessados, com conhecimentos técnicos, que partilham as vulnerabilidades que identificam (muitas vezes, procurando-as) de forma a informar as empresas de tecnologia e os consumidores. Chama-se "*zero day*" às vulnerabilidades que são divulgadas, mas que ainda não têm medidas de mitigação associadas.

5 A divulgação de vulnerabilidades depende em grande medida de iniciativas de *ethical hacking*, isto é, de atividades de investigadores que colocam à prova os sistemas, muitas vezes através de tentativas de intrusão. Essas atividades devem ser enquadradas legalmente e em Políticas de Divulgação Responsável de Vulnerabilidades, de modo a proteger judicialmente estes indivíduos e melhorar o processo de comunicação entre fornecedores, investigadores e utilizadores.

6 A revisão da Diretiva SRI promove medidas para a coordenação da divulgação destas vulnerabilidades, bem como a criação de um registo centralizado de vulnerabilidades a nível europeu. Em Portugal, o CNCS, juntamente com vários parceiros, tem procurado contribuir com propostas de trabalho para a constituição de uma Política de Divulgação Responsável de Vulnerabilidades no país.

PUBLICAÇÕES E NOTÍCIAS

O **DNS.PT** publicou o *Relatório Anual PTSOC 2020: Ano da ciberpandemia*, no âmbito das atividades do seu Centro de Operações de Segurança, o PTSOC, fazendo um balanço do ano de 2020, revelando, por exemplo, que houve 186 casos detetados de DNS Abuse durante o ano passado.

Em março, a **Comissão Nacional de Proteção de Dados**, publicou o seu *Relatório de Atividades 2019/2020*, onde mostra, entre outros aspetos, que em 2020 ocorreram 301 notificações de violações de dados, quando em 2019 tinham ocorrido 240.

A **ENISA – Agência da União Europeia para a Cibersegurança**, no dia 9 de abril, publicou o documento *Cybersecurity Certification Market Study*, no qual apresenta uma proposta dos passos metodológicos necessários para uma análise do mercado da certificação em cibersegurança das Tecnologias de Informação e Comunicação, contribuindo para a construção de um quadro europeu de certificação nesta área.

O **Conselho de Ministros**, entre os dias 12 de abril e 3 de maio de 2021, colocou em consulta pública o decreto-lei que "regulamenta o regime jurídico da segurança do ciberespaço, aprovado pela Lei n.º 46/2018, de 13 de agosto e define as obrigações decorrentes do Regulamento (UE) 2019/881 em matéria de certificação da cibersegurança".

O **INESC-ID**, a partir do dia 1 de maio, iniciou o desenvolvimento de um protótipo de deteção e análise do discurso de ódio no Twitter, visando a criação de mecanismos de identificação deste tipo de conteúdo, com a parceria do Centro Nacional de Cibersegurança e da Agência Lusa.

O **Centro Nacional de Cibersegurança**, em conjunto com a AP2SI e a 0xPOSEC, lançou uma *Call For Presentations*, que esteve disponível até ao dia 24 de maio, através da qual foi possível apresentar propostas para apresentações de ter técnico a realizar na Conferência CDAYS 2021. A adesão foi muito significativa. O CNCS agradece.

A conferência **C-DAYS 2021**, organizada pelo CNCS, irá realizar-se nos próximos dias 14, 15 e 16 de junho, na Alfândega do Porto, em formato *streaming*, aberto ao público. "Naturalizar competências" será o mote para os debates deste ano, o que significa tornar a cibersegurança numa preocupação natural e num "saber fazer" assimilado desde os primeiros anos de formação dos cidadãos e no modo de atuação das Empresas e da Administração Pública.

A CNCS pretende respeitar o direito à privacidade.
Os seus dados são tratados de forma sigilosa, sendo utilizados apenas para envio de informação do CNCS.

POLÍTICA DE PRIVACIDADE

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Observatório de Cibersegurança