Relatório Anual PTSOC 2020

"Ano da ciberpandemia"

.pt

Índice

CAPÍTULO 1

1.

Enquadramento

Em 2020, como resposta ao contexto de pandemia covid-19, o futuro chegou mais depressa e operou-se uma verdadeira revolução no digital, através da adoção massiva da tecnologia e do online para superar uma vastidão de exigências fundamentais decorrentes da situação de crise. O digital permitiu manter atividades e assegurar as necessidades mais básicas atenuando, desta forma, as devastadoras consequências económicas e sociais decorrentes da pandemia.

É, mais do que nunca, consensual que a Internet é um recurso vital e que a vida das sociedades modernas depende da tecnologia. No entanto, é importante reconhecer que o mundo digital é vulnerável e comporta riscos. Riscos que foram amplificados em 2020, registando-se o aumento muito significativo da atividade maliciosa no ciberespaço, a qual importa acompanhar.

Este primeiro relatório do Centro de Operações de Segurança do .PT – PTSOC – apresenta uma breve súmula dos principais acontecimentos e tendências que observámos em 2020 nos domínios da cibersegurança, fornecendo um maior conhecimento para endereçarmos os desafios que se antecipam para 2021.

CAPÍTULO 2

2.

Grandes ciberataques de 2020

janeiro

Travelex, uma rede britânica de câmbio de moedas que realiza 150 milhões de operações por ano em todo o mundo, foi alvo de um ciberataque de ransomware e obrigada a suspender a sua atividade, colocando offline os seus sites em 30 países.

fevereiro

Um erro de software no Portal das Finanças Dinamarquês, expôs informação pessoal de 1.26 milhões de Dinamarqueses, isto é, um quinto do total da população da Dinamarca. Esta vulnerabilidade, esteve exposta durante 5 anos (de 2015 a 2020), até ser descoberta.

março

A cadeia hoteleira Marriot, em abril, foi alvo de um ciberataque, tendo sido usadas por hackers credenciais de utilizadores internos para aceder aos sistemas e aplicações na cadeia hoteleira e exfiltrar informações pessoais dos mais de 5 milhões de clientes.

abril

A EDP, operadora energética portuguesa, foi alvo de um ciberataque que permitiu aos hackers exfiltrar mais de 30 TB de informação sensível da companhia.

maio

Nove milhões. Foi este o número de clientes da Easy-Jet que foram expostos a um ciberataque. Perante estes eventos, a EasyJet fez face a um processo na ordem dos 18 mil milhões de libras.

junho

Ransomware. esta foi a ciberameaça que afetou a Universidade da Califórnia (UCSF) em Junho e que a fez desembolsar um total de 1.14 milhões de dólares para reaver os seus dados.

julho

Elon Musk, Jeff Bezos, Joe Biden, Barack Obama, Bill Gates. Poderíamos estar a enumerar algumas das personalidades mais influentes da América. Mas não. Estas foram as pessoas que, após um ataque de phishing direcionado ao Twitter, viram as suas contas do Twitter serem controladas por agentes maliciosos.

Este ataque teve, na sua primeira hora um impacto financeiro de pelo menos 118 mil dólares.

agosto

A Intel, famosa fabricante de processadores, foi alvo de um Data Breach de onde fizeram parte mais de 20GB de documentos internos classificados como confidenciais.

setembro

O Hospital Duesseldorft foi alvo de um ransomware. Este ataque impossibilitou o hospital de receber uma paciente a necessitar de cuidados médicos urgentes. Consequentemente, esta paciente teve de ser transferida para outro hospital, 30km mais distante. Sendo o tempo crítico e crucial nestas situações, a paciente acabou, infelizmente, por falecer.

outubro

A International Maritime Organization, responsável pela segurança de embarque e prevenção da poluição marítima de navios, foi alvo de um ciberataque sofisticado que obrigou a organização a desligar os seus sistemas, deixando os seus serviços públicos inacessíveis.

novembro

A AstraZeneca foi alvo de um ciberataque com vista ao roubo de informações sobre as pesquisas desenvolvidas no âmbito da COVID-19. Acredita-se que este ciberataque tenha sido desenvolvido por Hackers localizados em Pyongyang, na Coreia do Norte. Os hackers fazendo-se passar por recrutadores no LinkedIn e no WhatsApp, enviavam a funcionários da AstraZeneca documentos maliciosos que dariam acesso aos sistemas internos da farmacêutica.

dezembro

SolarWinds, uma empresa americana de tecnologia de redes, com clientes pertencentes à Fortune 500, reconheceu que foi inserido malware nos updates de software da plataforma Orion.
A exploração ativa desta vulnerabilidade conduziu ao ciberataque de 2020, o qual figura, certamente, como um dos mais marcantes da história da cibersegurança, impactando 18 mil clientes nomeadamente a FireEye, a Microsoft, entidades governamentais americanas, entre outras.

CAPÍTULO 3

3.

Top ciberameaças em 2020

Campanhas de Phishing relacionados com o COVID-19

Associada à necessidade de acesso de informação sobre a pandemia COVID-19, o número de campanhas de phishing disparou. Assistimos a um aumento de phishing na ordem dos 600%, nomeadamente associado a ofertas de testes de rastreio, a apoios financeiros em virtude da crise ou mesmo fraudes relacionadas com edução à distância.

Ataques a trabalhadores à distância

2020 ficou marcado também pela adoção em massa de tecnologias que permitiram o trabalho à distância. A introdução destas novas tecnologias trouxe novas oportunidades para as organizações, mas também novos riscos. A utilização massiva da aplicação Zoom foi um dos casos mais citados com a descoberta de vulnerabilidades que permitiam a execução remota de vulnerabilidades (RCE).

Serviços Cloud

Face ao crescimento da adoção de tecnologias em cloud, diversos ciberataques, em 2020, mostraram que os serviços em Cloud podem ser comprometidos através de uma diversidade de técnicas. Não obstante, o maior risco na adoção da Cloud estar relacionado com a configuração incorreta dos acessos remotos a estes sistemas. Em 2020, vimos os cibercriminosos a explorar vulnerabilidades, nomeadamente associada à falta de uso de autenticação de múltiplos fatores, para aceder às ferramentas de gestão e, desta forma, controlar os sistemas das organizações.

Ransomware, a maior ameaça

Claramente, 2020 foi o ano em que assistimos a mais ataques utilizando este modus operandi. Os meios utilizados são mais sofisticados, os pedidos de resgate tornaram-se maiores e novas técnicas de extorsão começaram a ser experimentadas pelos cibercriminosos.

CAPÍTULO 4

O que vimos no .PT em 2020

Principais Indicadores

3
Auditorias de Segurança

368
Eventos Reportados no Canal Interno

Top 3 ameaças

Casos detetados de DNS Abuse – **186**

Enumeração da zona .PT – **24**

Desvio anormal no comportamento de utilizadores – **23**

369
Eventos de Segurança

123
Eventos Reportados abuse@dns.pt

O que vimos no .PT em 2020

Malware

81
Malware Bloqueado

100%
PC's Protegidos

56
Aplicações Potencialmente Indesejadas Bloqueadas

249
Acessos internos a Websites maliciosos bloqueados

22
Exploits Bloqueados

O que vimos no .PT em 2020

Phishing/Spam

645.142
E-mails Recebidos

10.48%
Emails de Spam/Malware

62.57%
Aumento do n.º de emails com malware

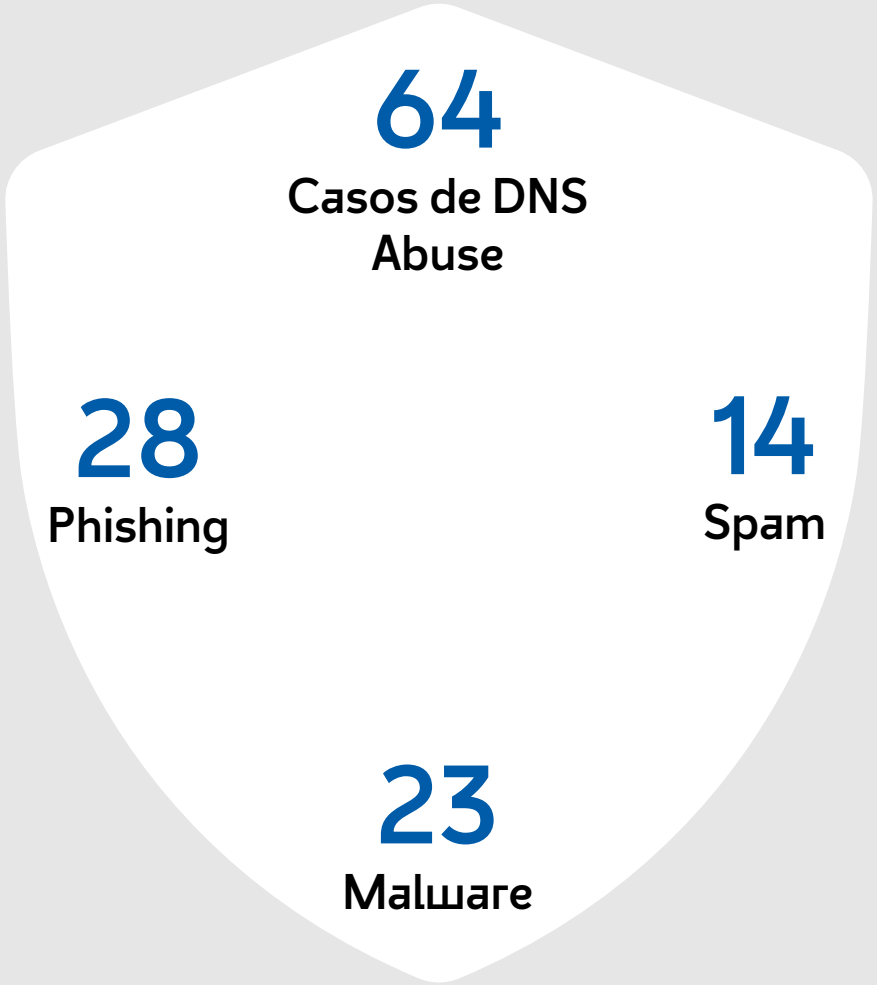
2%
E-mails que falharam política DMARC

5%
E-mails que falharam política DKIM

61%
E-mails que falharam política SPF

O que vimos no .PT em 2020

DNS Abuse



Com a revisão das regras de registo em .pt foi introduzido o conceito de DNS Abuse.

Um nome de domínio registado em .pt pode ser classificado como DNS Abuse quando suportar uma ou mais das seguintes atividades: Malware, Botnets, Phishing, Pharming e Spam.

O que vimos no .PT em 2020

Webcheck

121
Visitas em média por dia

19.644
Testes realizados

66.5%
Páginas web testadas com HTTPS

19.7%
Páginas web testadas com DNSSEC

10.2%
Páginas web testadas com HSTS

47.0%
Correio electrónico testado com SPF

29.8%
Correio electrónico testado com STARTTLS

O que vimos no .PT em 2020

Ações de sensibilização

82.14%
Média no Quiz

3
Ações de sensibilização realizadas

9
E-mails de sensibilização interna

CAPÍTULO 5

5.

Cooperação e Estratégia

Assembleia da República | Em 2020, em cooperação com o .PT foram desenvolvidos os esforços para a implementação de DNSSEC nos domínios do Parlamento, bem como foram reforçadas as medidas de segurança no seu correio eletrónico.

.PT | Reforçada a parceria do .PT com a Autoridade Nacional de Cibersegurança (CNCS) com a entrada no programa Panorama.

Webcheck.pt | Dinamização da plataforma que resulta da iniciativa conjunta do .PT e do CNCS, que tem o objetivo de promover a adoção de boas práticas e standards que contribuem para garantir a segurança, integridade e confidencialidade nas comunicações via internet.

.PT | Foi definida e publicada a política que define formalmente o modo de partilha do ficheiro de zona de .pt com os seus parceiros.

Conselho da União Europeia (UE) | Pela primeira vez, a UE aplicou medidas restritivas a entidades singulares e coletivas na sequência do apoio à realização de vários ciberataques a entidades Europeias.

Conselho da União Europeia (UE) | Apresentação da nova estratégia europeia para a cibersegurança e ainda a revisão da Diretiva NIS (2.0)

CAPÍTULO 6

Para onde olhar em 2021

"Os ataques direcionados aos teletrabalhadores vão ser mais frequentes"

Em 2020, os cibercriminosos fizeram do phishing a sua principal cyberweapon, como porta de entrada para acesso aos sistemas e informações das organizações. Para além dos fatores tradicionais (baixo custo e facilidade de execução) o contexto social de pandemia agravou a motivação para esta prática.

O teletrabalho veio para ficar. Em 2021, com o previsível estender da situação social de pandemia e das medidas, mais ou menos, restritivas de confinamento, prevê-se que o teletrabalho continue a ser uma realidade das organizações na garantia das suas atividades.

Neste alinhamento, espera-se que os ataques direcionados a teletrabalhadores tenham um crescimento tanto em número como em sofisticação.

Para onde olhar em 2021

"O alvo dos ataques de Ransomware será a exfiltração de informação"

Casos recentes de Ransomware ilustram que esta atividade é altamente impactante para as organizações e extremamente lucrativa para os cibercriminosos.

Contudo, em 2020, começámos a assistir a uma tendência de alteração no modus operandi dos ataques de Ransomware, onde o alvo passou a ser a exfiltração de informação, isto é, o roubo e consequente pedido de resgate ao invés da simples encriptação e pedido de resgate.

É assim de esperar que, em 2021, o ransomware e atividades derivadas continuem a ser uma das maiores ciberameaças para as organizações.

Para onde olhar em 2021

"As pessoas passaram a ser o novo perímetro das organizações"

Em resposta ao contexto de crise pandémica Covid-19, muitas organizações tiveram a urgente necessidade de transitar ou dar os primeiros passos no mundo digital, em particular, através de serviços prestados na Cloud.

Infelizmente, a par da urgência na adoção do digital, verificou-se um aumento de sistemas vulneráveis nestes ambientes, principalmente devido a configurações inadequadas de segurança.

Em 2021, prevendo-se a continuidade do contexto de pandemia, iremos assistir a um aumento significativo dos ataques a sistemas em Cloud. Com a adoção crescente desta tecnologia e do teletrabalho as organizações deixaram de ter o seu tradicional perímetro físico. As pessoas passaram a ser o novo perímetro das organizações. Será, pois, estratégico, nos próximos anos, o reforço das atividades de gestão de identidades e de acessos privilegiados.

Para onde olhar em 2021

"A dimensão dos ataques de negação de serviço a atingir records em largura de banda"

A expectativa do 5G é grande. As pessoas querem um futuro mais conectado e mais automatizado.

Embora o 5G permita que as organizações acelerem a sua transformação digital e criem novas experiências na relação com os cliente como, por exemplo, a possibilidade de condução autónoma de veículos. Esta tecnologia também aumenta exponencialmente a superfície de ataque. Teremos mais dipositivos interconectados no mundo digital, com uma largura de banda muito superior. Surgem, pois, novos ciberriscos para organizações.

Em 2021, espera-se que a dimensão dos ataques de negação de serviço (DDoS) atinja, não só, records em largura de banda assim, bem como, em número de dispositivos IoT vulneráveis e explorados por botnets presentes no mundo digital.

Citação do ano

“With great flexibility comes great responsibility”

Dennis Okpara, Chief Security Architect & DPO at IDEE GmbH

Referências

1 | Acronis, Acronis Cyberthreat Report 2020, https://dl.acronis.com/u/rc/ШР_Acronis_Cyber_Threats_Report_2020_EN-US_201201.pdf

2 | Observatório de Cibersegurança, Relatório de Cibersegurança em Portugal, Dezembro 2020, https://шшш.cncs.gov.pt/content/files/relatorio_sociedade2020__observatoriocibersegurança_cncs.pdf

3 | Checkpoint Research, Cybersecurity Report 2020, https://шшш.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

4 | TechHQ, Six cybersecurity trends heading our шay in 2021, https://techhq.com/2020/12/six-cybersecurity-trends-heading-our-шay-in-2021/

5 | Comissão Europeia, Nova Estratégia da UE para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais, Dezembro 2020, https://ec.europa.eu/commission/presscorner/detail/pt/ip_20_2391

ptsoc

Produção: janeiro 2021
Grafismo: .pt