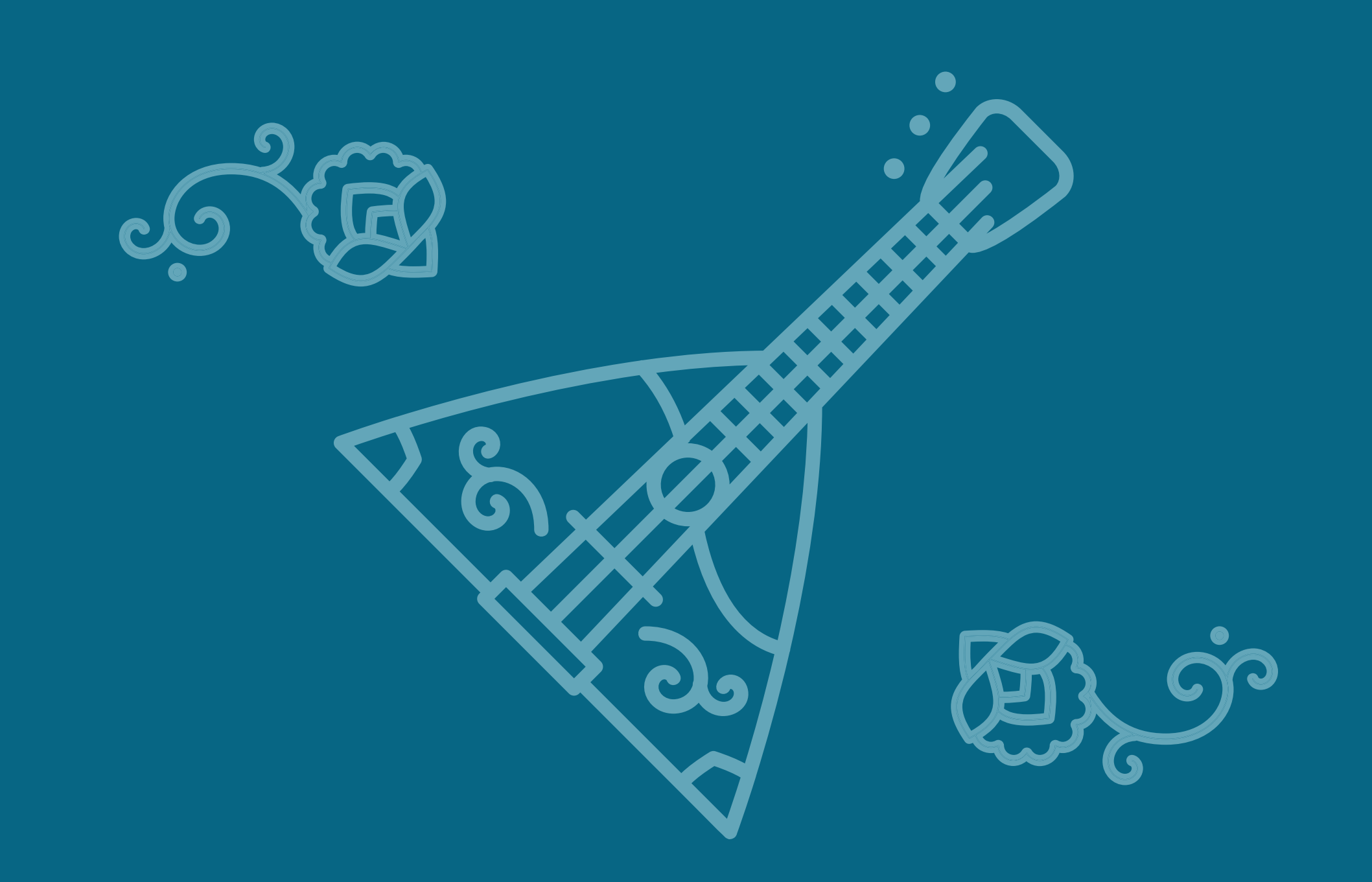
RELATÓRIO CENTR JAMBOREE 2018

30 de maio a 1 de junho - Moscovo, Rússia

Council of European National
Top-Level Domain Registries

ÍNDICE



INTRODUÇÃO

Figura 1 – CENTR Jamboree 2018

De 30 de maio a 1 de junho decorreu o CENTR Jamboree 2018, em Moscovo. Mais de 150 participantes e seis grupos de trabalho (administrativo, I&D, jurídico, marketing, técnico e segurança) reuniram-se para discutir as tendências no mundo dos ccTLD's. O Jamboree é um dos principais eventos do CENTR. Decorre durante três dias e promove a partilha de experiências entre os grupos de trabalho, que habitualmente se reúnem de forma independente.

O evento iniciou com uma apresentação do anfitrião, o Coordination Center for TLD RU/РФ, que apresentou alguns dos seus dados: 6 milhões de domínios, 45 registrars e 25 colaboradores. Sobre o negócio, referiu que atingiram um crescimento de 2,5% e que o preço de venda de domínio e de renovação aumentou 70%, sendo que o preço não se alterava desde 2007. O .RU referiu ainda que introduziu a transferência de nomes de domínio em bloco, permitindo a aquisição parcial de portefólio. Estão ainda a trabalhar no Registry Lock Service e num novo procedimento para libertar nomes de domínio expirados, sobretudo para fazer face ao *drop-cacthing*.

Disponibilizamos nos pontos que se seguem algumas das conclusões que destacamos das sessões em que o .PT participou.

A IMPLEMENTAÇÃO DO RGPD NOS CCTLD'S

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS E O IMPACTO NOS CCTLD'S

No grupo jurídico o grande foco foi para o Novo Regulamento Geral de Proteção de Dados (RGPD). Inclusive, numa das sessões foram apresentadas e discutidas cinco questões, em grupos compostos por seis pessoas que depois apresentaram aos restantes as suas conclusões:

1. Procedimentos para tratar pedidos de acesso a dados pessoais
Aqui a análise recaiu na dupla perspetiva possível: acesso pelo próprio titular ou por terceiros. A maioria dos registries presentes criou endereços de email e estabeleceu internamente procedimentos para o efeito, que passam pela definição de quem recebe o email (tipicamente uma equipa constituída pela área jurídica e técnica e, por vezes, o DPO), pelo prazo para resposta e pelos critérios que devem ser avaliados. No .PT este trabalho ainda não foi realizado de forma tão exaustiva. Uma nota que foi feita é que, em todo o caso, se deve evitar o envio de cartões de identificação para provar o que quer que seja, se possível deve-se sempre recorrer ao ID *number* de registo.

2. Formação
Comum foi a ideia que deve ser dada formação, mas progressivamente já que ainda há muito que interiorizar e entender.

Também aqui duas vertentes complementares: RGPD e princípios e regras enformadoras e, depois, o negócio em si e as implementações concretas feitas por cada Registry. O CENTR vai realizar um breve *webinar* sobre a primeira parte que disponibilizará aos seus membros.

3. Novo Whois, como lidar com as alterações
Aqui, e salvo o caso espanhol onde apenas foram suprimidos alguns contactos (princípio da minimização), todos os registries informaram ter alterado a informação que agora é visível. Na maior parte dos casos - exceção de .es e .eu - os dados pessoais deixam simplesmente de ser exibidos. O caso de Portugal, com a solução "*consent based*", tem também poucos seguidores.

4. Prazo de retenção
Na maior parte dos casos a opção é 10 anos (indexada à responsabilidade contratual). No caso do .es é 12 anos (decorrente da lei) e no .be é para sempre.

O CENTR afirmou que apaga os dados das inscrições nos eventos, por exemplo, ao fim de uma semana.

5. Procedimentos técnicos adotados
Os necessários à operacionalização, estando ainda em curso na maior parte dos casos. Os registries com certificação ISO 27000

estão numa posição mais, digamos, confortável já que, sobretudo ao nível da segurança da informação, já tinham várias implementações previamente concluídas.

Conclusões: Muito trabalho feito, ainda muito por fazer. O dia a dia vai ser determinante para afinar procedimentos e não há visões claras.

IDENTIDADES DIGITAIS E ESTRUTURAS DE CONFIANÇA NO REGISTO DE DOMÍNIOS

Vários ccTLD's estão a implementar soluções deste tipo, por exemplo .dk, .nl, .cz e .ee. Começaram a trabalhar nisso um pouco alavancados pelos respetivos governos quando estes implementaram soluções de ID orientadas aos cidadãos. Isto na sequência da publicação em 2016 do regulamento comunitário eIDAS - electronic IDentification, Authentication and trust Services.

O .DK apresentou os trabalhos que tem vindo a desenvolver no sentido de diminuir a fraude de identidades no registo de domínios. Numa primeira fase, o Registry efetuou uma integração com o sistema de identificação nacional, o NemID, equivalente ao Cartão de Cidadão português, que faz com que, no caso de cidadãos nacionais, seja mais fácil o controlo automático da veracidade dos dados no registo. O NemID é adoptado por 98% dos cidadãos dinamarqueses com mais de 15 anos. Para as entidades que não são nacionais, o Registry criou um sistema automático de análise e deteção de dados falsos. Este sistema reconhece os dados submetidos pelo registrar e, baseado num conjunto de métricas e algoritmos de aprendizagem automáticos, deteta se os dados têm caraterísticas duvidosas. Se forem detetados dados duvidosos, o Registry contacta o registrant e pede para validar os mesmos, sendo que se forem identificados dados falsos ou o registrant não responder

os domínios são removidos. Este sistema levou a uma redução significativa do número de domínios fraudulentos no .DK, aumentando assim a confiança do TLD.

O .ee utiliza uma solução idêntica, o .nl utiliza o sistema Connectis (www.connectis.nl/eidas) e o .cz tem um single *sign on service* desde 2010 que vai ser integrado, já no próximo mês de julho, com a solução a lançar pelo Governo.

Foi ainda apresentado o ID4me como uma solução de login com o nome de domínio. Para implementar o ID4me é necessário ter um parceiro neutro, instalar software e diversas configurações, realizar testes e suportar DNSSEC.

Em todos estes casos pensamos estarem na mesa opções próximas da nossa Chave Móvel Digital. Uma nota final para dizer que em relação ao caso Dinamarquês não é possível um nacional registar um domínio sem usar o respetivo NemID.

ANONIMIZAÇÃO E PSEUDO-ANONIMIZAÇÃO DE DADOS

As técnicas de anonimização e pseudo-anonimização de dados têm vindo a ser bastante discutidas, principalmente com a entrada em vigor do RGPD. Estas referem as medidas que são efetuadas por parte dos registries para anonimizar os dados de clientes de forma a que estes não possam ser recuperados. As técnicas de pseudo-anonimização diferem das anteriores, já que os dados podem ser recuperados usando as técnicas corretas. Vários ccTLD's referiram a utilização destas técnicas, devido à necessidade de anonimizar os dados após a entrada em vigor do RGPD. Para o .PT é importante ouvir falar sobre estas temáticas, nomeadamente para se ter uma visão mais alargada sobre como implementar estas soluções.

A QUESTÕES DOS CONTEÚDOS

A discussão sobre a questão dos conteúdos já não é novidade, nomeadamente no que diz respeito aos conteúdos ilegais e à remoção de nomes de domínios. Esta questão foi novamente abordada neste fórum, sendo que dois dos participantes na discussão, o .nl e o .dk, afirmaram ter um procedimento próprio para este efeito. Seguem ambos caminhos idênticos, orientados não para a totalidade de situações que se podem subsumir neste âmbito, mas apenas para os casos de domínios que suportam lojas online falsas. Para os restantes casos em que têm conhecimento de conteúdos ilícitos os mesmos são tratados à luz de políticas de *notice and take down*. À critica que policiam a internet responderam que não, apenas policiam identidades, já que as remoções resultam de tentativas de contacto com os titulares dos domínios em causa que, por regra, não resultam e dão lugar à remoção do domínio (suspendem por 30 dias e só depois removem definitivamente). Em ambos os casos são pró-ativos, ou seja, verificam a zona com periodicidade procurando identificar este tipo de casos (recorrendo a uma solução de DeMap) e os resultados são publicados num relatório público. Para além disso fazem verificações ao WHOIS e analisam os próprios conteúdos: qualidade das fotos, não indicação de contactos fiáveis ou apenas de endereços de email tipo Gmail ou Hotmail, grandes descontos, etc.

Questões de fundo mantêm-se: deve um ccTLD ter intervenção a este nível? Não é suposto gerir apenas a infraestrutura de suporte ao serviço? Por outro lado, ainda que remova os domínios a história não vai acabar por aqui e os infratores encontrarão soluções alternativas quase imediatas.

O CENTR informou que está a preparar um documento sobre o papel que os registries podem assumir no controlo de conteúdos ilegais.

QUESTÕES E DISCUSSÕES TÉCNICAS

LOCAL ANYCAST

O .PT participou num painel sobre a implementação de Local Anycast em diversos ccTLD's e apresentou a sua solução de Local Anycast, bem como a sua evolução com este sistema. O projeto Local Anycast .PT tem como objetivo implementar uma nuvem de servidores secundários de .PT, com a metodologia Anycast, para proteger a internet, em Portugal, em cenários de ataques de negação de serviço (DDoS) contra o serviço DNS em .PT. Segundo esta metodologia estão, neste momento, operacionais dois servidores secundários de .PT.

Para além do .PT participaram no painel o .NL, o .BE e o .CZ. Todas as soluções de Local Anycast apresentadas recorrem, de uma forma ou de outra, às mesmas tecnologias e sistemas e são todas quase gratuitas para as entidades recetoras, sendo que alguns registries adquiriram o equipamento e outros pediram à entidade recetora o mesmo. No geral a solução do .PT está em linha com as restantes e demonstra possibilidade de crescimento.

ROTAÇÃO DA CHAVE KSK

A rotação da chave KSK da root zone é um tema em grande destaque, ou não fosse este potencialmente impactante para a segurança e estabilidade da internet e de um número ainda incerto de utilizadores. O tema foi mais uma vez mencionado também neste fórum de discussão. De recordar que a ICANN suspendeu o processo, que estava previsto para dia 11 de outubro de 2017, porque havia indicadores de que esta poderia afetar mais utilizadores do que o considerado aceitável. Após alguma discussão na comunidade de DNS, e tendo em conta o feedback dessa mesma comunidade e uma análise mais aprofundada dos dados disponíveis, a ICANN decidiu avançar com a rotação a 11 de outubro de 2018.

HARDWARE SECURITY MODULE

Está a ser desenvolvido um novo HSM (Hardware Security Module) que difere dos restantes por ter todos os esquemáticos de funcionamento e desenho públicos, de forma a criar um hardware transparente. O HSM (Hardware Security Module) é um equipamento físico que guarda e gere chaves de segurança digitais que servem para encriptação e autenticação. Esta nova solução, ainda no início do desenvolvimento, apresenta-se como uma boa solução, mas demonstra, para já, problemas de rapidez para ser usado por um TLD com um número considerável de domínios assinados, como é o caso do .PT.

COMO USAR O DNS PARA GERAR SEGURANÇA NA INTERNET

O .IT propõe adicionar registos que mapeiam os sistemas internos de casas e empresas que automaticamente se registam no DNS, criando assim uma estrutura de segurança e confiança nos mesmos. Esta solução tem vindo a ser falada na comunidade nos últimos tempos e tem vindo a posicionar-se como uma nova fonte de receita para os ccTLD's.

O .BE apresentou as alterações que fez recentemente ao seu sistema de monitorização, de forma a que este seja mais preciso e a que não tenha tantos falsos positivos. Este trabalho demorou algum tempo a ser concretizado, mas, segundo o Registry, o sistema ficou bastante mais robusto e fiável.

O .CA também deu o seu contributo e apresentou os últimos desenvolvimentos do seu sistema de registo, o FURY. Ao longo dos últimos anos o .CA refez o seu sistema de registo, que se encontra atualmente em fase de promoção e comercialização. Nos últimos meses foram adicionadas mais algumas características. Foi ainda adicionado o primeiro TLD de uma entidade externa ao .CA, o .SX, tendo havido algumas complicações no processo de transição mas, no final, foi concluída com sucesso.

DIRETIVA NIS

O Parlamento Europeu adotou, a 6 de julho de 2016, a proposta de Diretiva NIS (network and information security - segurança das redes e da informação), a primeira legislação ao nível da União Europeia sobre cibersegurança, que estabelece um conjunto de medidas para prevenir incidentes cibernéticos na Europa. O .PT tem vindo a acompanhar a evolução do novo quadro legislativo e regulamentar, decorrente da aprovação e entrada em vigor de vários diplomas a nível europeu e que terão impacto na nossa atividade, como é o caso da Diretiva NIS.

O .DK apresentou alguns desenvolvimentos na transição da Diretiva na Dinamarca e o impacto para o ccTLD. Esta transição elenca um conjunto de requisitos para a identificação dos operadores de serviços essenciais, por exemplo um TLD é um operador de serviços essenciais quando gere mais que 500.000 domínios ou, ainda, um operador de um servidor autoritativo com mais de 100.000 SLD. É também nesta transição que são identificadas as situações que requerem a comunicação dos incidentes às Autoridades de Segurança, por exemplo um TLD com disponibilidade do serviço inferior a 100%, ou, ainda, um autoritativo com disponibilidade do serviço por um período superior a 6h. É ainda necessário comunicar à autoridade quando existe perda de integridade, autenticidade e confidencialidade que afete mais de 10.000 utilizadores.

OUTRAS QUESTÕES RELEVANTES NO ÂMBITO DO FUNCIONAMENTO DE UM CCTLD

MODELO DE MATURIDADE: PARTICIPAÇÃO DO .PT

No âmbito do CENTR, foi desenvolvida uma iniciativa conjunta pelos membros .DE, .BE, .AT, .NL e .CH, designada de Modelo de Maturidade de Segurança (CMM-SMM). Este modelo foi desenvolvido tendo por base modelos de referência já existentes, normas e melhores práticas, e pretende-se, com esta iniciativa, avaliar a maturidade de segurança em 5 domínios (Gestão, Prevenção, Deteção, Resposta e Recuperação) e 21 subdomínios da segurança dos ccTLD's e identificar onde estes podem melhorar neste âmbito.

Durante o CENTR Jamboree, o .BE apresentou os resultados obtidos e os principais pontos de melhoria para os ccTLD's participantes. As melhorias identificadas estão relacionadas com a gestão da cadeia de fornecimento, a gestão de configurações e automatizações, a engenharia de software e desenvolvimento seguro, a gestão de logs e da monitorização e, ainda, a melhoria dos mecanismos de deteção de incidentes de segurança.

INTERNET DAS COISAS E OPORTUNIDADES

Ao nível da Internet das Coisas e oportunidades por ela geradas, durante o evento foram discutidos os riscos de segurança e privacidade associados aos dispositivos e aparelhos que, funcionando em rede, foram concebidos e desenvolvidos para resolver problemas quotidianos, no plano físico e lógico. Clarificou-se que muitos destes objetos não têm efetivamente ligação à internet, mas têm implementados sistemas de comunicação entre objetos, objetos-humanos, humanos-objetos. No que respeita à segurança e privacidade, o recurso a estes dispositivos apresenta inúmeros problemas e desafios relacionados com:

1 - Rastrear comportamentos;
2 - Estabelecer *profilings*;
3 - Geolocalização;
4 - Violações da liberdade individual;
5 - Aplicação do princípio da territorialidade da lei, entre outros.

Alguns registries estão a desenhar soluções tecnológicas para garantir a segurança destes objetos, diminuir o seu impacto negativo e potenciar os seus benefícios.

EXERCÍCIO PRÁTICO:
SIMULAÇÃO DE UM CIBERATAQUE

No decorrer do CENTR Jamboree, o .PT participou num exercício de simulação de um ciberataque à infraestrutura de uma organização de extração de petróleo e gás, organizado em parceria com a Kaspersky Lab. O objetivo deste exercício passava por treinar os decisores e as equipas de segurança para responderem da melhor forma possível aos incidentes que iam surgindo, num cenário caótico, onde o tempo e o crescente número de incidentes criavam pressão nos jogadores.

Figura 2 – Exercício de simulação de um ciberataque

Participaram no exercício cinco equipas que competiram entre elas para obter o maior retorno com o menor gasto possível. O cenário iniciou-se com a descoberta de que os servidores da companhia estavam vulneráveis ao Shellshock e decorreu ao longo de cinco turnos. A vulnerabilidade identificada poderia já ter sido explorada e podia já ter sido posta em causa a infraestrutura. Tendo isto em consideração, os jogadores podiam optar por corrigir a vulnerabilidade, sensibilizar os colaboradores ou mudar palavras-passe, sendo que cada uma destas opções tinha custos monetários e temporais diferentes.

Algumas conclusões tiradas do exercício são que os ciberataques afetam as receitas das organizações e, por isso, devem ser endereçados pela gestão de topo, a cooperação entre o negócio e as equipas técnicas é essencial para uma maior eficácia da cibersegurança e o orçamento disponibilizado para a segurança é normalmente inferior à receita que se arrisca perder.

Figura 3 – Apresentação do .PT

O .PT fez ainda uma apresentação sobre a próxima reunião do grupo de trabalho CENTR Security, que se vai realizar em Lisboa, no dia 29 de outubro.

ESTATÍSTICAS DOS TLD'S

Aqui realçamos o foco generalizado na análise de dados e estatísticas associadas ao registo e manutenção de nomes de domínio por parte dos registries. O CENTR prepara e disponibiliza, no seu website, estatísticas sobre o mercado de nomes de domínio, estatísticas essas que foram também apresentadas no CENTR Jamboree. Neste aspeto destacamos os seguintes dados:

Mercado Global de TLD: 1.4% de crescimento dos TLD's a nível mundial;

Na Europa a distribuição de registos entre ccTLD's é mais uniforme do que nos restantes continentes que têm normalmente ccTLD's grandes em número de registos e outros consideravelmente menores;

O .com mantem-se como o gTLD com maior crescimento, continuando a crescer na Europa em contraposição aos restantes gTLD's;

Considerando os membros do CENTR, verifica-se que os residentes preferem o registo no ccTLD local (54%), seguido do .com e do .eu;

Todos os ccTLD's do CENTR estão a crescer, apresentando um crescimento médio de 3.8%. A desaceleração no crescimento está a diminuir e isto é justificado pela diminuição na taxa de remoção de domínios (2017). O que se verifica é que quem tem uma taxa de remoção superior tem uma taxa de crescimento inferior;

Relativamente aos preços, em média o preço por domínio nos ccTLD's europeus varia entre 4€ e 8€. Nos ccTLD's mais pequenos, o preço situa-se entre 4€ e mais de 12€. Existe uma pequena relação entre preço e crescimento, verificando-se que quem apresenta um maior crescimento, o preço situa-se nos 4€. Aqueles com um crescimento mais lento apresentam um preço mais elevado. O preço para renovação, em média, é ligeiramente superior ao preço de registo.

Figura 4 – Crescimento por país:
PT continua a ser um dos ccTLD's que mais cresce

DADOS PARA PERCEBER OS NOSSOS MERCADOS E IMPULSIONAR NEGÓCIOS

Vários registries têm sentido a necessidade de renovar a sua imagem e o modo de comunicação com os seus registrars e clientes. Antes de avançarem para uma nova estratégia, esses registries realizaram estudos de mercado e tentaram perceber as razões que justificam a escolha de um TLD em detrimento de outro (por exemplo o .com é muitas vezes escolhido para comércio internacional), uma vez que se considera que esta é uma informação fundamental para definir qual a nova abordagem que terão sobre o mercado. Neste contexto, os registrars são o veículo privilegiado para chegar aos clientes e, portanto, devem ter acesso ao máximo de informação e acompanhamento possível.

O .ie percebeu que tinha de simplificar o processo de registo de nomes de domínio e, por essa razão, criou um conjunto de animações para os seus registrars, com o intuito de serem usadas por estes no âmbito da sua atividade e serem disponibilizadas nos seus websites (p. ex. uma animação de como se regista um domínio). O Registry tentou maximizar o seu apoio aos registrars e, assim, os maiores registrars conseguiram, inclusivamente, realizar campanhas na rádio. No entanto, alguns registrars não estiveram dispostos a fazer campanhas em conjunto, apenas individualmente. O próprio Registry participa em diversos eventos para promover o registo de nomes de domínio, por exemplo, eventos organizados especificamente para micro/pequenas empresas e *start ups* (p. ex. procuram explicar que os clientes confiam mais nas empresas que usam um email corporativo em detrimento de um Gmail ou Outlook). Participam em muitos destes eventos juntamente com os seus registrars, sendo que são convidados os registrars que mais vendem.

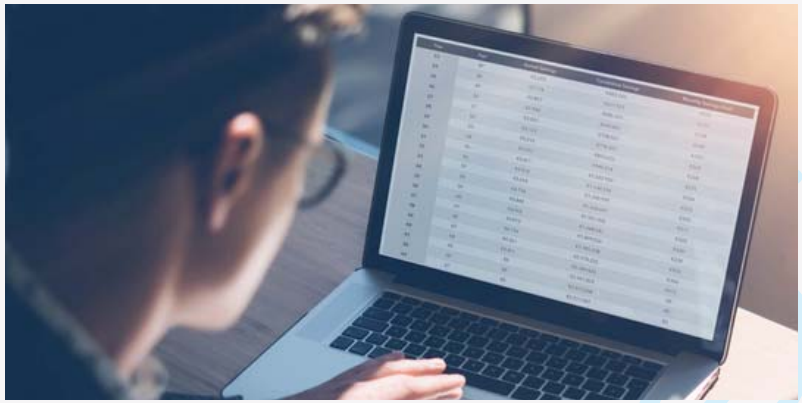
Por sua vez, a Nominet realizou um trabalho sério e aprofundado de análise da informação associada aos nomes de domínio registados sob .uk. Começaram por categorizar os nomes de domínio registados e, para o efeito, contrataram uma equipa de analistas temporária que ficou responsável por perceber para que propósito os domínios estavam a ser usados (agricultura, serviços, indústria, etc.). Os resultados obtidos foram partilhados com os registrars, sendo que um dos maiores, após conhecer esta informação, fez uma campanha televisiva, tendo-se, inclusivamente, verificado

um aumento do número de novos registos nesse registrar. Da análise efetuada resultaram conclusões importantes relativamente à retenção de nomes de domínio, uma vez que foi efetuado um trabalho de previsão (com recurso a algoritmos específicos) da probabilidade de renovação dos nomes de domínio já registados sob .uk (esta análise tem 81% de correção). Esta informação mostrou-se muito relevante pois, consoante a probabilidade de um nome de domínio ser renovado, decidir-se-ia se valeria ou não a pena investir em campanhas direcionadas ou alertas para renovação. A análise realizada teve, ainda, uma componente importante de segurança, considerando que a equipa de análise usou técnicas (com recurso a algoritmos) para encontrar palavras que pudessem indiciar que um determinado website estava a ser usado para fins ilícitos. Após esta identificação era realizada uma breve "investigação" e os domínios podiam acabar por ser removidos.

DROP-CATCHERS E DOMÍNIOS PREMIUM

Definição de conceitos:

- **Drop-Catcher:** indivíduo ou empresa que regista nomes de domínio imediatamente após estes ficarem livres para registos, seja porque não foram renovados ou porque o registrant perdeu interesse no mesmo.
- **Snapcatching:** indivíduos ou empresas que, lançando várias *queries «create domain»*, identificam e registam vários nomes que se encontram disponíveis para registo.
- **Snipecacthing:** indivíduos ou empresas que lançam apenas uma única *query «domain create»* para registar um domínio em particular, normalmente porque o domínio em causa apresenta um valor acrescido.



Razões subjacentes ao drop-catching:

- Construir um portefólio de domínios (poderá não ser necessariamente para venda);
- Registar domínios apelativos que permitem gerar muito tráfego e, consequentemente, apresentam uma elevada rentabilidade;
- Fazer da venda de domínios o seu negócio e, nestes casos, há uma preferência pelo registo de nomes genéricos, uma vez que o mercado de potenciais compradores é maior;
- Após o domínio ser removido por falta de renovação, registam de imediato o domínio para o vender ao anterior titular.

Posicionamentos contra ou a favor do drop-catching:

O .de mostra-se a favor, uma vez que, pagando-se pelo registo do nome de domínio e pelos recursos técnicos utilizados, deve, então, funcionar exclusivamente o princípio da prioridade registral (*first come, first served*). O .fr também não se mostra desfavorável ao *drop-catching*, no entanto reconhece já ter implementado um conjunto de mecanismos técnicos que permitem mitigar alguns dos seus efeitos perniciosos. Outros registries manifestaram-se desfavoráveis considerando que esta atividade levanta vários problemas em termos de legitimidade para o registo de nomes, aumentando os conflitos em matéria de nomes de domínio.

MARKETING | COMUNICAÇÃO

Estes fóruns de partilha de experiências são particularmente interessantes para as equipas de marketing e comunicação. Novas ideias são sempre bem-vindas e, neste capítulo, conseguimos sempre trazer algumas, que necessitam obviamente de ser adaptadas ao nosso contexto e mercado.

A maioria dos registries têm como missão, muitas vezes integrada nos seus estatutos, a dinamização da internet nos respetivos países. Muitos deles têm programas específicos nesta área: Netidee do .AT, que apoia projetos e atividades de empresas e indivíduos que impulsionem o desenvolvimento da internet; Internetopoli do .it, que tem como objetivo promover a cultura digital nas escolas; Afnic Foundation for Digital Solidarity do .fr para onde vão 90% dos lucros da AFNIC; no .CA os lucros são usados também na comunidade; o .NK apoia projetos sobre competências em TI; e o .NZ realiza campanhas sobre copyright, privacidade e segurança. No caso do .PT, em 2018 estamos a afetar uma parte dos recursos destinados a ações de dinamização e promoção do uso da internet em Portugal a iniciativas e projetos que nos cheguem da comunidade em geral. O tema genérico é o das “Competências Digitais”. Com esta iniciativa pioneira o .PT reforça a aposta e o contributo, que desde há muito tem sido efetivo, para a promoção da internet a nível nacional.

Outras iniciativas realizadas pelos ccTLD's, e partilhadas durante o evento, que considerámos particularmente interessantes são as abaixo descritas:

- **NASK, .pl:** criação de um folheto para registrars e de uma animação para registrants sobre as vantagens de registar nomes de domínio sob .pl; produção de vídeos educativos para jovens (o que é um nome de domínio, razões para registar, como registar);
- **NIC.AT:** organização do evento de comemoração do aniversário e Registry Day (30 anos .at; 20 anos NIC.AT e Stopline; 10 anos CERT). O .PT também comemora 30 anos este ano;
- **Registro.it:** realização de um roadshow sobre a digitalização das PMEs italianas;
- **AFNIC, .fr:** elaboração de um guia para PMEs com 50 dicas para construir uma presença online; organização do 3º Fórum AFNIC;
- **SIDN, .nl:** criação de uma ferramenta de sugestão de nomes de domínio no site. O .PT já tem uma ferramenta deste género no seu site, mas está a equacionar desenvolvê-la e melhorá-la aquando do lançamento da nova imagem corporativa e, consequentemente, do novo site.

USAR O MARKETING E A COMUNICAÇÃO PARA CONTRUIR MARCAS

Aqui contámos com o contributo de três registries: Nominet, CIRA e AFNIC.

A Nominet, Registry do .uk, referiu que está a alavancar a área de produtos de cibersegurança, afirmando que já são bastante conhecidos enquanto Registry e, por isso, o foco agora é promover os restantes produtos. Como estratégia de marca apresentou três grandes áreas: DNS Cibersecurity Services, Registry Services e Emerging Technology. O objetivo é transmitir a mensagem de que a Nominet opera no centro da infraestrutura da internet e está habilitada para fornecer outros produtos/serviços para além do registo de nomes de domínio. Neste âmbito produziram o vídeo "Nominet Cyber Security":
https://www.youtube.com/watch?v=ae2mrCISsLI

Por seu lado, a CIRA tem como objetivo promover o registo do .CA, para tal tenta apelar às emoções dos canadianos com campanhas onde utilizam slogans como: "Choose Canada. Choose .CA", ".CA your Canada online" ou "The internet needs more Canada". A CIRA tem vindo a focar-se nos millennials, para tal criaram a campanha Digital Me (https://cira.ca/digital-me), onde utilizam influenciadores (desportistas, artistas reconhecidos) para chegar ao público alvo. Os resultados foram 537.000 novos domínios registados em 2017, sendo o melhor ano de sempre. Os lucros da CIRA são usados na comunidade e, por isso, o objetivo é também transmitir a

mensagem de que “If you buy a .CA, the money gets back to you”.

Já a AFNIC foca-se em três eixos de comunicação: Registry experiente e fiável; domínios e muito mais; e organização sem fins lucrativos. O objetivo é promover a AFNIC enquanto Registry, mas também posicionar o .fr como o expert da presença online (não apenas como Registry). Para transmitir a mensagem que para eles é chave, “Tenha sucesso com o .fr”, têm vindo a promover diversos produtos/serviços: .fr Watch, .fr Lock, Reussir en France, .fr Rush. Além disso, estão a firmar parcerias com *website builders* muito conhecidos em França. A AFNIC referiu ainda que 90% dos seus lucros vão para a Afnic Foundation for Digital Solidarity e que irá lançar, ainda em junho, um “Brand TLD’s white book”.

Em género de conclusão, assistimos aqui a três focos de comunicação diferentes: a Nominet está focada no objetivo (diversificação da oferta), a CIRA nas alterações de mercado (millennials) e a AFNIC em como apresentar a marca aos consumidores (*expert* da presença online).

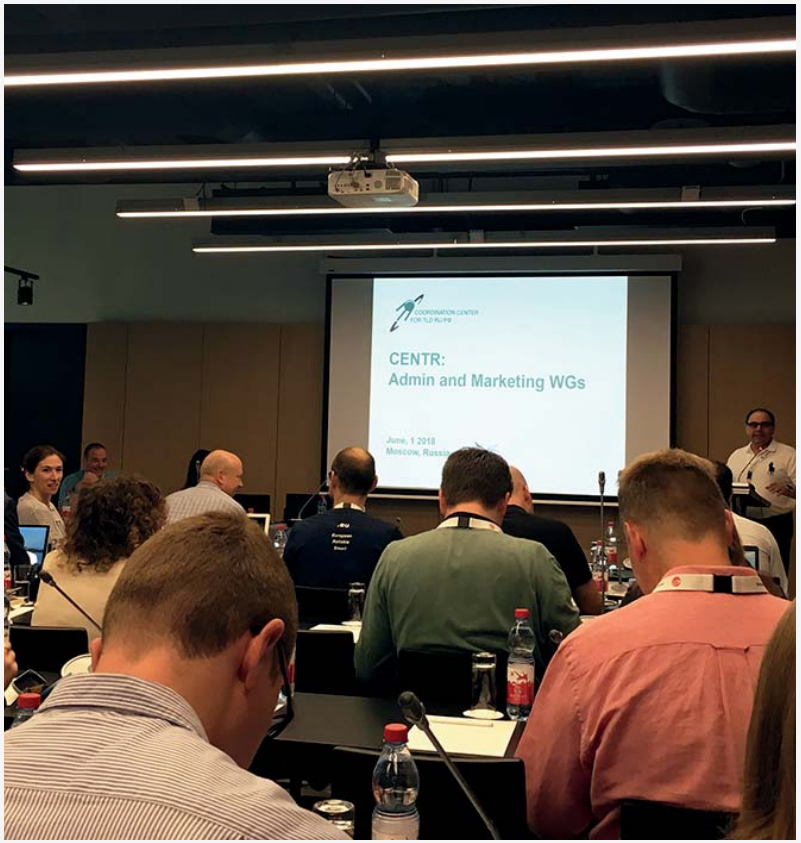


Figura 5 – Reunião CENTR Admin/Marketing

dns.pt
dnssec.pt
facebook.com/dns.pt
pt.linkedin.com/in/dnspt

Produção: junho 2018
Grafismo: dns.pt