bilingual edition

ptsoc{news}

Selos para a Maturidade Digital

3 perguntas a Nuno Cavaco

Privacidade e o DNS (Parte II: as soluções)
por João Damas

04

Digital Maturity Seals

3 questions to Nuno Cavaco

Privacy and the DNS (Part II: the solutions)
by João Damas

.pt

Selos para a Maturidade Digital

As organizações públicas e privadas, nomeadamente as PMEs que têm investido na cibersegurança, podem agora ver reconhecido publicamente esse esforço através da ostentação de um Selo de Maturidade Digital (SMD), obtido após um processo de certificação (CMD).

A cibersegurança é um dos quatro pilares em que assenta essa CMD, acompanhada pela privacidade e proteção de dados pessoais, sustentabilidade e acessibilidade. Todos terão uma especificação técnica, com requisitos assegurados pelo Organismo Nacional de Normalização/Instituto Português da Qualidade (ONN/IPQ) e pelo Instituto Português de Acreditação (IPAC). As normas da cibersegurança e da acessibilidade já foram publicadas pelo IPQ, enquanto as regras da privacidade e da sustentabilidade aguardam publicação em breve, segundo Nuno Cavaco, coordenador da Transformação Digital do Tecido Empresarial no programa Portugal Digital (ver "3 Perguntas a...").

Coexistem três níveis de certificação (bronze, prata e ouro), a que se junta um Selo Digital Global após "a certificação nas quatro dimensões específicas, mediante a obtenção de uma pontuação

Digital Maturity Seals

Public and private organizations, namely SMEs that have invested in cybersecurity, can now see this effort publicly recognised through the display of a Digital Maturity Seal (DMS), awarded after a certification process (MDC).

Cybersecurity is one of the four pillars this MDC is based on, together with privacy and protection of personal data, sustainability and accessibility. All of these will have a technical specification, with requirements ensured by the National Organization for Standardization/Portuguese Institute of Quality (ONN/IPQ) and the Portuguese Institute for Accreditation (IPAC). The cybersecurity and accessibility standards have already been published by IPQ, while privacy and sustainability rules should be published soon, according to Nuno Cavaco, coordinator of Enterprises' Digital Transformation at the Portugal Digital programme (see '3 Questions to...').

Three certification levels coexist (bronze, silver and gold), to which a Global Digital Seal is added after 'certification in the four specific dimensions, after obtaining a minimum score', states the Portuguese Certification Association (APCER), one of the certifying entities in

mínima", segundo a Associação Portuguesa de Certificação (APCER), uma das entidades certificadoras na cibersegurança, juntamente com a Bureau Veritas. O selo global caduca ao perder-se a certificação num dos quatro pilares.

Desde um primeiro "webinar" em setembro de 2021 para apresentar a iniciativa, a APCER começou "a ter manifestações de interesse e pedidos de esclarecimentos sobre a norma e respetivo processo de certificação", que prosseguiu com "reuniões e sessões de esclarecimentos junto de muitas organizações. Recentemente com os acontecimentos ocorridos no âmbito da cibersegurança, a procura intensificou-se", assegura Francisco Pimenta, Business Developer de IT Security da APCER.

A instituição espera "ter todos os tipos de empresas e organizações, sejam públicas ou privadas. Esta norma de cibersegurança foi criada para ser facilmente adaptável a qualquer tipo de negócio e dimensão de empresa/organização. O que está em jogo é a segurança e prevenção de ataques cibernéticos, que têm tendência para aumentar substancialmente ao longo dos anos, e as empresas devem apostar na continuidade do seu negócio recorrendo à implementação e certificação de acordo com estes referenciais normativos",

cybersecurity, along with Bureau Veritas. The global seal expires when certification on one of the four pillars is lost.

After a first webinar in September 2021 where the initiative was presented, APCER began 'receiving manifestations of interest and queries on the standard and its certification process', which continued with 'meetings and briefings held with many organisations. Recently, with the events that have occurred in the area of cybersecurity, the demand increased', assures Francisco Pimenta, IT Security Business Developer at APCER.

The institution hopes to 'include all kinds of companies and organisations, be they public or private. This cybersecurity standard is designed to be easily adaptable to any type of business and company/organisation size. What is at stake is the security and prevention of cyberattacks, which have shown a tendency

aconselha aquele responsável.

Os requisitos para a cibersegurança estão assegurados pela norma DNP TS 4577 (ver pág. 8) e foram os primeiros a serem definidos.

Nessa certificação, a obtenção do selo está indexada ao WebCheck, a ferramenta online da Associação DNS.PT (.PT) e do Centro Nacional de Cibersegurança (CNCS) para "promover a adoção de boas práticas e standards que contribuam para garantir a segurança, integridade e confidencialidade nas comunicações através da Internet". Aliás, o .PT posicionou-se para ser uma entidade certificada no nível Ouro, já tendo entregue a candidatura para a certificação.

Os principais benefícios dos SMD na cibersegurança passam pelo "aumento contínuo da segurança da informação e prevenção de ataques nas redes informáticas", no sentido de garantir a "confidencialidade, integridade e disponibilidade" para reduzir os riscos das ciberameaças.

"As empresas cada vez mais assumem a cibersegurança como tema inevitável", explica Nuno Cavaco, a que acresce o potencial para assim obterem uma maior

to increase substantially over the years; companies should invest in the continuity of their business by resorting to implementation and certification according to these normative benchmarks', he advises.

The requirements for cybersecurity are covered by standard DNP TS 4577 (see page 8) and were the first ones to be set.

This certification's seal is indexed to Webcheck, Associação DNS.PT (.PT) and the Portuguese National Cybersecurity Centre (CNCS)'s online tool to 'promote the adoption of good practices and standards that contribute to ensure security, integrity and confidentiality in communications through the Internet'. In fact, .PT has positioned itself as a Gold-level certified entity, having already submitted the application for certification.

DMS's main cybersecurity benefits are the 'continuous increase of information security and prevention of attacks on computer networks' in order to ensure 'confidentiality, integrity and availability' to reduce the risks of cyber threats.

'More and more, companies are seeing cybersecurity as an unavoidable subject,

notoriedade da marca, assente na diferenciação, credibilidade e maior competitividade.

A emissão dos selos é coordenada pela Imprensa Nacional-Casa da Moeda (INCM), cuja Plataforma de Certificação, informa sobre o processo de candidatura, as entidades certificadoras, certificadas, parceiras e outras entidades intervenientes, como a Global Enabling Sustainability Initiative (GeSI), garantindo-se um reconhecimento mútuo com o Digital with Purpose desta organização.
Segundo Nuno Cavaco, "conferir às empresas e organismos públicos a possibilidade de, ao obterem a sua certificação de maturidade digital, também serem reconhecidas no modelo GeSI, e vice-versa, traduz-se em benefícios que potenciam a visibilidade nacional e internacional das organizações, mas também reforça os níveis de exigência das práticas digitais a implementar, estimulando a inovação como motor da transformação digital".

Todas as organizações de quaisquer setores de atividade, tipologia e dimensão vão poder certificar-se consoante os seus interesses, prioridades e relevância para o negócio, e podem ser financiadas pelo Plano de Recuperação e Resiliência

explains Nuno Cavaco, adding to it the potential to achieve greater brand awareness based on differentiation, credibility and greater competitiveness.

The issue of the seals is coordinated by the Portuguese Mint and Official Printing Office (INCM), whose Certification Platform, provides information on the application process, certifying entities, certified entities, partner entities and other stakeholders, such as the Global Enabling Sustainability Initiative (GeSI), ensuring mutual recognition with this organisation's Digital with Purpose.

According to Nuno Cavaco, 'also giving companies and public entities the possibility of, when obtaining their digital maturity certification, being recognised under the GeSI model, and vice versa, translates into benefits that enhance the organisations' national and international visibility, while also strengthening the standards of digital practices to be implemented, stimulating innovation as a driver of digital transformation.'
All organisations, from any activity sector, typology and size, will be able to obtain a certification according to their business interests, priorities and relevance, and can be financed by the

(PRR). “Temos 30 milhões de euros reservados para apoiar a certificação e as primeiras 15 mil certificações vão ter apoio financeiro”, assegurou André de Aragão Azevedo, então secretário de Estado da Transição Digital, no evento

Recovery and Resilience Plan (RRP). ‘We have 30 million euros set aside to support the certification and the first 15 000 certifications will be granted financial support’, assured André de Aragão Azevedo, then Secretary of State for

Benefícios até €30 milhões

Os SMDs integram-se no Plano de Ação para a Transição Digital. Em conjunto com a avaliação da maturidade digital das organizações, os benefícios dos selos traduzem-se em:

• minimizar a exposição ao cibercrime (certificação de cibersegurança);

• aumentar o potencial de interagir com novos clientes (certificação de acessibilidade);

• melhorar a capacidade de gerir dados sensíveis (certificação de privacidade);

• contribuir para o combate às alterações climáticas (certificação de sustentabilidade); e

• incrementar a notoriedade e o negócio.

Up to €30 million in benefits

DMSs are integrated in the Digital Transition Action Plan. Together with the assessment of organisations' digital maturity, the seals’ benefits include:

• minimise exposure to cybercrime (cybersecurity certification);

• increase the potential to interact with new customers (accessibility certification);

• improve the capacity to manage sensitive data (privacy certification);

• being a contributor to the fight against climate change (sustainability certification); and

• increase awareness and revenue.

em que o Modelo Nacional de CMD foi apresentado.

A tarefa deve estar terminada até ao terceiro trimestre de 2025 porque "os SMDs são uma medida enquadrada no PRR e como tal tem associada metas concretas", nota Nuno Cavaco. "No pressuposto que cada empresa se certifica nas quatro dimensões, estaríamos a falar de 3.750 empresas".

Também Francisco Pimenta considera que se "atingirmos perto das 15 mil certificações propostas pelo Portugal Digital, será um sucesso para todas as partes envolvidas". Apesar de não ser "possível quantificar uma duração média ou um custo médio de momento, uma vez que estamos muito no início do lançamento desta norma", os selos acabam por revelar a maturidade digital das organizações.

Cibersegurança pioneira

Cada área de intervenção foi elaborada em conjunto com uma entidade parceira. Para a cibersegurança foi escolhido o Centro Nacional de Cibersegurança, na acessibilidade a Agência para a Modernização Administrativa, a privacidade ficou com a Comissão Nacional para a

Digital Transition, at the event in which the MDC's National Model was presented.

The task must be completed by the third quarter of 2025 because 'DMSs are a measure within the RRP and, as such, are associated to specific goals', notes Nuno Cavaco. 'Assuming that each company is certified in the four dimensions, we would be talking about 3 750 companies.'

Francisco Pimenta also believes that if 'we reach close to the 15 000 certifications proposed by Portugal Digital, it will be a success for all parties involved'. Although it is not 'possible to, at the moment, quantify an average duration or cost, since we are still at the very early stages of this standard's launch', the seals are a testament to the digital maturity of organizations.

Pioneering cybersecurity

Each intervention area was developed with a partner entity: for cybersecurity, the Portuguese National Cybersecurity Centre was chosen; for accessibility, the Agency for Administrative Modernisation; for privacy, the National Data Protection Authority and for sustainability, the Directorate-General for Economic

Proteção de Dados e, por fim, na sustentabilidade, a Direção-Geral das Atividades Económicas. Segundo o regulamento da marca SMD, estes parceiros coordenados pelo ONN/IPQ devem manter atualizado o conhecimento das tendências europeias e internacionais; transpor o conhecimento mais recente para a realidade nacional; informar o IPQ sobre eventuais evoluções técnicas para a atualização de documentos normativos; apoiar esse instituto em questões técnicas; participar no modelo de governação do SMD e, por fim, apoiar a capacitação dos auditores (formação).

No primeiro domínio concretizado - a cibersegurança -, foram certificadas as empresas Cycloid (bronze), Sisqual (prata) e SportTV (também prata).

Nuno Ferreira Pires, CEO da Sport TV, alertou em comunicado para a necessi-

Activities. According to the DMS's regulation, these partners, coordinated by the ONN/IPQ, must keep their knowledge of European and international trends up to date, transpose the latest knowledge to the national reality, inform the IPQ of any technical developments in order to update normative documents, support this institute on technical issues, participate in the governance model of the DMS and support the training of auditors.

In the first domain - cybersecurity -, several companies were awarded certification, namely Cycloid (bronze), Sisqual (silver) and SportTV (also silver).

Nuno Ferreira Pires, CEO of Sport TV, stated that there is a need to have a 'real value matrix associated with a maximised digital transition. Those who have not yet started their digital transition, or those who do not yet consider this a strategic theme, run serious risks of not operating in the future market or, should they be able to operate, lose much of their competitive edge.'

Although the initiative certifies national companies, it can be incorporated into a broader model with standards validated by international entities, as is the case

dade de se ter uma "real matriz de valor associada a uma transição digital maximizada. Quem não iniciou já a sua transição digital, ou quem não considere ainda este um tema estratégico, corre sérios riscos de não operar no mercado futuro ou, operando, perder grande parte da sua competitividade".

Embora certifique as empresas a nível nacional, a iniciativa pode englobar-se num modelo mais alargado com normas validadas por entidades internacionais, como sucede com a GeSI. Será assim possível identificar entidades estrangeiras pela sua maturidade digital para estabelecer compromissos comerciais mais confiáveis.

Os modelos de maturidade digital têm vários anos. De forma simples, podem caracterizar-se por fornecer um "framework", uma estrutura conceptual "para medir a maturidade de um programa de segurança e orientação sobre como alcançar o nível seguinte". Num outro modelo, estabelecem-se cinco dimensões, divididas em 28 sub-temas, para obter 179 critérios individuais. O objetivo, como nos SMDs, é definir o grau de maturidade digital da organização. ■

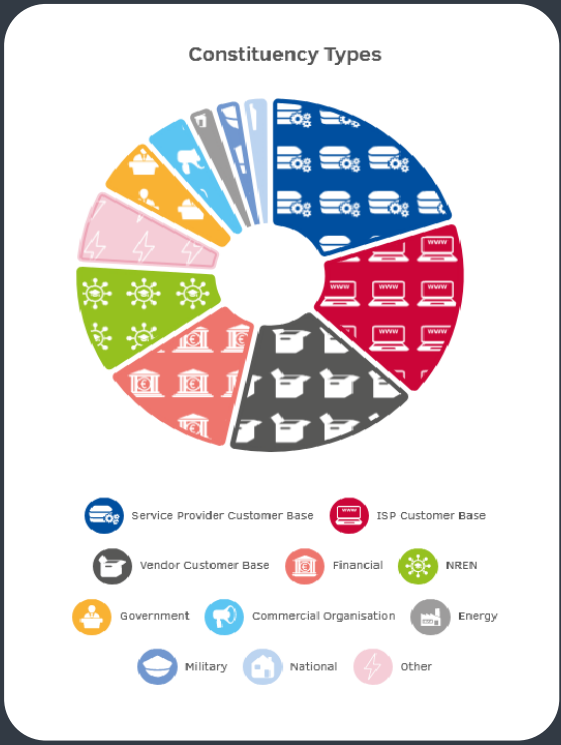
with GeSI. It will thus be possible to identify foreign entities by their digital maturity to establish more reliable business commitments.

Digital maturity models are a few years old, now. Simply put, they provide a framework, a conceptual structure for 'measuring the maturity of a security program and guidance on how to reach the next level.' In another model, five dimensions are established, divided into 28 sub-themes, to obtain 179 individual criteria. The goal, as with DMSs, is to define an organisation's degree of digital maturity. ■

CSIRTs

As Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) estão reguladas pela diretiva NIS (enquanto se espera pela NIS 2). A NIS obriga à definição de - pelo menos - um CSIRT nacional por país, como sucede com Portugal, mas o número total de CSIRTs portugueses já atinge as 42 equipas.

Computer Security Incident Response Teams (CSIRTS) are regulated by the NIS Directive (while we wait for NIS 2). NIS requires the definition of - at least - one national CSIRT per country, as with Portugal, but the total number of Portuguese CSIRTS already reaches 42 teams.



The Global Risks Report

95% dos problemas na cibersegurança das empresas podem ser atribuídos a erros humanos e 43% de todas as falhas são de ameaças internas (intencionais ou acidentais), assegura a nova edição deste relatório do World Economic Forum, que coloca a cibersegurança como o principal risco tecnológico acelerado pela pandemia.

95 % of all companies' cybersecurity issues are traced to human error and 43 % of all failures are internal threats (intentional or accidental), ensures the new edition of this report by the World Economic Forum, which places cybersecurity as the main technological risk accelerated by the pandemic.

3

Nuno Cavaco

Coordenador da Transformação Digital para as Empresas no Programa Portugal Digital
Coordinator - Enterprises' Digital Transformation at the Portugal Digital programme

1. Como está a ser recebida a divulgação pública dos Selos de Maturidade Digital (SMD), nomeadamente na componente da cibersegurança?

A cibersegurança é um tema absolutamente crítico e deve ser encarada como uma prioridade imediata das organizações.

A aceleração da transição digital da sociedade e das empresas resultante, em grande parte, da situação pandémica atual, veio expor as organizações a uma nova realidade de riscos, cujos impactos podem ter graves consequências para os seus negócios.

A criação do modelo nacional de certificação em maturidade digital, inclui quatro normativos de boas práticas (cibersegurança, acessibilidade, privacidade e sustentabilidade), com três níveis de exigência (bronze, prata e ouro).

1. How is public information about the Digital Maturity Seals (DMS) being received, namely in the cybersecurity world?

Cybersecurity is an absolutely critical issue and should be seen as an immediate priority for organisations.

The acceleration of society and companies' digital transition, greatly due to the current pandemic situation, exposed organisations to a new reality regarding risks, whose impacts can have serious consequences for their businesses.

The creation of the national certification model in digital maturity includes four standards of good practices (cybersecurity, accessibility, privacy and sustainability), with three rating levels (bronze, silver and gold). The implementation of these standards ensures that organisations comply with these good practices, allowing them, regarding the specific case of cybersecurity, to minimise the risks of cybercrime.

The regulations on cybersecurity and accessibility have already been published by the IPQ (Portuguese Institute of Quality), with two certification

A implementação destas normas, confere às organizações o garante de que estão em conformidade com estas boas práticas, permitindo-lhes, no caso concreto da cibersegurança, minimizar os riscos de cibercrime.

Atualmente, os normativos da cibersegurança e da acessibilidade já foram publicados pelo IPQ (Instituto Português da Qualidade), existindo duas entidades certificadoras acreditadas em cibersegurança pelo IPAC (Instituto Português de Acreditação) e três empresas certificadas em cibersegurança, uma com selo bronze e duas com selo Prata.

As empresas cada vez mais assumem a cibersegurança como tema inevitável e a receção à divulgação pública dos SMD tem sido bastante expressiva, com várias manifestações de interesse em implementar os respetivos normativos.

2. Esperam ter mais organizações públicas ou privadas a aderir aos SMDs?

As quatro dimensões de certificação referem-se a preocupações transversais que tanto respeitam ao setor privado como ao público.

bodies accredited in cybersecurity by the IPAC (Portuguese Institute for Accreditation) and three companies certified in cybersecurity, one with a Bronze seal and two with a Silver seal.

Companies are increasingly seeing cybersecurity as an inevitable subject to address and the public disclosure of DMSs was quite expressive, with several companies showing an interest in implementing these regulations.

2. Do you expect to have more public or private organisations joining the DMSs?

The four certification dimensions refer to cross-sectoral concerns, regarding both private and public sectors.

It is a matter of priorities, in which each organisation defines the theme that, at the moment, brings it the most value, taking into account its exposure to risk and the nature of its activity.

Cybersecurity aims to minimise the risk of cybercrime; accessibility includes practices that broaden digital inclusion, allowing greater interaction with new users/customers; privacy focuses on improving the ability to

É uma questão de prioridades, em que cada organização define o tema que lhe aporta mais-valor no momento, tendo em conta a sua exposição ao risco e a natureza da sua atividade.

A cibersegurança visa a minimização do risco de cibercrime; a acessibilidade inclui práticas que aumentam a inclusão digital, permitindo aumentar a interação com novos utilizadores/-clientes; a privacidade tem como foco a melhoria da capacidade de gerir dados sensíveis; e a sustentabilidade tem como propósito contribuir, por via do digital, para uma economia mais verde.

É indiscutível que na sua complementaridade, os quatro selos são um meio para as organizações adotarem boas práticas digitais, aumentando a sua notoriedade, bem como a confiança nas cadeias de valor e com a sociedade.

Estamos convictos que a mobilização será expressiva e independente do setor e da dimensão das organizações, pois os três níveis de maturidade digital (bronze, prata e ouro) permitem não deixar ninguém para trás e promover a adoção gradual dos requisitos.

manage sensitive data; and sustainability aims to digitally contribute to a greener economy.

It is indisputable that, in their complementarity, the four seals are a means for organisations to adopt good digital practices, increasing their notoriety as well as trust in value chains and society itself.

We believe that mobilisation will be significant and independent of the sector and size of organisations, given that the three levels of digital maturity (bronze, silver and gold) encompass everyone and promote the gradual adoption of the requirements.

3. How will the initiative's success be measured?

As an RRP measure, its direct success is associated with the ability to meet the goal of issuing 15 000 seals.

However, underlying the creation of a monitoring model for this measure, which is expected to have a dashboard component monitoring its implementation, indicators could be defined which, while safeguarding the privacy of information, can assess results and

3. Como será medido o sucesso da iniciativa?

Sendo uma medida PRR, o sucesso direto da mesma está associado à capacidade de cumprir a meta de emissão de 15 mil selos.

Contudo, subjacente à criação de um modelo de monitorização da medida, que se perspetiva ter uma componente de "dashboard" de acompanhamento da sua execução, poderão ser definidos indicadores que, salvaguardando a privacidade da informação, são capazes de avaliar resultados e impactos.

Importa referir que os SMD são um processo que induz à adoção contínua de práticas a serem auditadas periodicamente, mantendo assim válidas as certificações emitidas, o que por si também constitui evidência de que as organizações reconhecem o valor dos SMD. ■

impacts. It should be noted that the DMSs are a process that leads to the continued adoption of practices that require periodic auditing, in order to keep the valid certifications issued, which in itself also constitutes evidence that organisations recognise the value of DMSs. ■

Privacidade e o DNS (Parte II: as soluções)

João Damas

Investigador sénior, APNIC Labs
Consultor do .PT
Senior Researcher, APNIC Labs
Consultant .PT

Na primeira parte desta série, descrevemos os problemas em torno de como o protocolo DNS, tendo sido concebido há já algum tempo, expõe dados ou metadados relativos à atividade de um utilizador, algo crescentemente tido como indesejável e considerado como um relevante risco de segurança e privacidade na Internet dos dias de hoje. Quando navegamos para um nome de domínio, o sistema DNS entra em ação para obter o endereço IP para possibilitar que alcancemos o serviço pretendido. Neste sistema, existem dois elementos que, durante as operações, irão sempre ter de conhecer todas as informações do DNS:

- o local/stub resolver, geralmente o sistema operativo ou a app;
- o resolver recursivo que irá executar o processo de resolução do DNS para o utilizador final.

Na maioria das implementações de DNS atuais, cada consulta realizada para obter o IP para o serviço pretendido inclui o nome de domínio completo.

Por exemplo, uma pesquisa por "ptsoc.pt.pt" irá enviar o domínio completo e o nome do subdomínio para o servidor .pt que, na realidade, irá fornecer a mesma resposta se a pesquisa for por "pt.pt", que conteria menos dados. Para resolver esse problema, surgiu um

Privacy and the DNS (Part II: the solutions)

In the first part of this series we described the problems around how the DNS protocol, having been designed a long time ago, exposes data or metadata from a user's activity that is increasingly seen as undesirable and considered a relevant security and privacy risk in today's Internet. When we navigate to a domain name, the DNS system comes into action to get the IP address to make possible we reach the service we pretend. In this system there are two elements that will always need to know all the DNS information during the operations:

- the local/stub resolver, usually the operating system or the app;
- the recursive resolver that will perform the process of DNS resolution for the end user.

In most of the current DNS implementations each query performed to get the IP for the service we pretend includes the complete domain name.

For instance, a lookup for "ptsoc.pt.pt" will send the complete domain and subdomain name to the server for .pt, which

novo mecanismo para reduzir a quantidade de fugas de dados, intitulado minimização QNAME.

Em cada etapa do processo de resolução, o mecanismo de minimização QNAME apenas realiza a consulta com a quantidade mínima de informações necessárias para fornecer a resposta correta. Com este mecanismo, os servidores .com apenas veriam uma consulta para "slack.com" e não para "ptnog.slack.com", reduzindo assim a exposição do utilizador à mineração de dados. Outro risco de segurança e privacidade que se tornou cada vez mais relevante nos dias que correm é a transmissão de dados de DNS em texto simples - o que significa que qualquer agente entre estes dois pontos pode ver e alterar os dados. Esta preocupação aumentou ainda mais com o crescimento de resolvers abertos/públicos de DNS populares, como 8.8.8.8, 1.1.1.1 ou 9.9.9.9 os quais estão, tipicamente, a várias redes de distância do utilizador e aglomeram muitos dados interessantes.

Para resolver este problema, o IETF tem estado a trabalhar em protocolos que encriptam a comunicação, o transporte. O mais popular destes tem sido o DoH, DNS sobre HTTPS (DNS over HTTPS), principalmente graças ao apoio de criadores de navegador. O DoH não só

in reality will provide the same answer if asked for "pt.pt", which would contain less data. To address this issue, a new mechanism emerged to reduce the amount of data leakage in named QNAME minimization.

The QNAME minimization mechanism, in each step of the resolution process will only query with the minimum amount of information it needs to provide the correct answer. With this mechanism, the .com servers would only see a query for slack.com and not ptnog.slack.com, hence reducing the user exposure to data mining. Another security and privacy risk which had become increasingly more relevant in these days are the transmission of DNS data in clear text. Which means that any agent in the middle of these two points can see and change the data. This became an even bigger concern with the growth of popular DNS open/public resolvers, like 8.8.8.8, 1.1.1.1 or 9.9.9.9, which are typically several networks away from the user and agglomerate a lot of interesting data.

To address this issue the IETF has been working on protocols that encrypt the communication, the transport. The most popular of these has been DoH, DNS over HTTPS, mainly thanks to the support from browser creators. DoH not

encripta as comunicações nos pacotes, como também esconde o fluxo de dados como parte do tráfego web HTTPS mais abundante, dificultando não só conseguir ver o que está nos dados, como também bloquear a utilização do mecanismo sem bloquear o tráfego HTTPS regular. Esta propriedade é vista como um benefício por alguns, mas também como um sério problema por outros; redes de empresas ficam, de repente, impossibilitadas de aplicar as suas regras normais de tráfego às suas redes internas, com o potencial de permitir que maus agentes se escondam nesse tráfego.

O trabalho também está a mostrar sinais de progresso, para permitir que o Doh consiga trabalhar sobre QUIC, o transporte selecionado para HTTP/3, ampliando os mecanismos definidos pelo DoH a esta nova versão de protocolo. Outra opção, até agora com menos apoiantes, é a DoT, DNS sobre TLS (DNS over TLS), que também encripta os dados no tráfego de DNS mas utiliza uma porta dedicada, permitindo assim um maior controlo sobre que tráfego é permitido numa determinada rede. Ainda não se sabe qual o protocolo que será mais utilizado, mas a direção que o desenvolvimento de protocolo, assim como o desenvolvimento de DNS, irá tomar é clara: a partir de agora, todos os protocolos terão de ter em consideração a privacidade de dados. ■

only encrypts the communications in the packets, it also hides the data stream as part of the more abundant HTTPS web traffic making it very hard not only to see what the data is but also to block the usage of the mechanism without blocking regular HTTPS traffic. This property is seen as a benefit by some but also as a serious problem by other parties, for instance by enterprise networks which suddenly cannot apply their normal traffic rules on their internal networks, with the potential for bad actors to hide in that traffic.

Work is also progressing in extending DoH to work over QUIC, which is the selected transport for HTTP/3, extending the mechanisms defined by DoH to this new protocol version.

Another option, which so far has less support, is DNS over TLS, DoT, which also encrypts the data in the DNS traffic but uses a dedicated port, therefore enabling more control over what traffic is allowed in a given network. Which protocol will be most used is unknown but it is clear what the direction for protocol development, and therefore DNS development is, and that is that all protocols will now have to take data privacy into account. ■

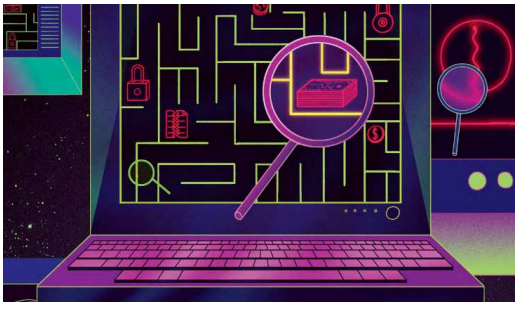
DNS4EU

A Comissão Europeia quer um novo sistema de resolução do DNS. Sob a sigla DNS4EU, a proposta visa contrariar a hegemonia norte-americana neste domínio e obter uma maior segurança e privacidade para os utilizadores, bloqueando sites com conteúdos ilegais. Mas o eurodeputado Patrick Breyer está contra por poder resultar numa "Euro-Net ao estilo chinês", com riscos de censura online, quando "o próprio bloqueio de DNS é facilmente contornado".

The European Commission wants a new DNS resolution system. Under the acronym DNS4EU, the proposal aims to counter the US hegemony in this area and achieve greater security and privacy for users by blocking websites with illegal content. However, MEP Patrick Breyer is against it, as it could result in a 'Chinese-style Euro--Net', with risks of online censorship, when 'block access is easy to circumvent by changing DNS servers'.

Bounty Everything

As plataformas de "bug bounty" pagam a informáticos pela descoberta de falhas ou de vulnerabilidades nos sistemas. Este relatório da Data & Society analisa "os riscos e inseguranças para os hackers como trabalhadores temporários e como estes programas de recompensas dependem de trabalhadores vulneráveis para corrigirem" as falhas. Sem vínculos ou garantias, ajudam a segurança informática numa enorme insegurança laboral. "Este modelo pode ironicamente perpetuar um mundo cheio de vulnerabilidades", pelo desejo das empresas se ilibarem de responsabilidades.

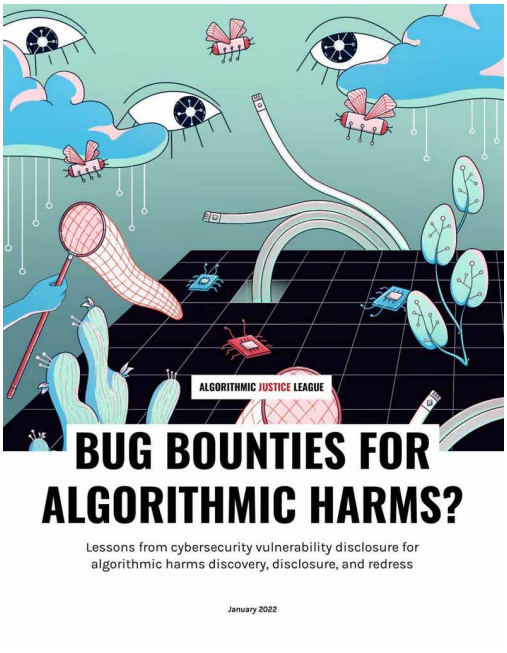


Bug bounty platforms pay programmers to expose faults or vulnerabilities in the systems. This Data & Society report analyses 'the risks and insecurities for hackers as gig workers, and how bounty programs rely on vulnerable workers to fix' the flaws. Without ties or guarantees, they help computer security in a huge labour insecurity. 'Ironically, this model can perpetuate a world full of bugs', as companies want to clear themselves of responsibilities.

Bug Bounties For Algorithmic Harms?

A Algorithmic Justice League analisa neste documento como os programas de "bug bounty" podem servir para ir mais além da cibersegurança e detetarem ou mitigarem "danos algorítmicos" em diferentes áreas, como os inevitáveis enviesamentos, assegurando um pagamento justo aos participantes nestas iniciativas.

In this document, the Algorithmic Justice League analyses how bug bounty programs can serve to go beyond cybersecurity and detect or mitigate 'algorithmic harms' in different areas, such as the inevitable biases, ensuring fair payment to participants in these initiatives.



Study on Domain Name System (DNS) abuse

Uma visualização anual mostra o tamanho e a influência dos diferentes registos de país ("country code Top Level Domains" ou ccTLD) como o .pt. Neste caso, o tamanho dos registos reflete a extensão territorial do país, num mapa com fronteiras inesperadas.

Domain Name System (DNS) abuse seeks to use domain names or the DNS protocol to carry out harmful or illegal activities. This study notes that this has been a 'frequent and serious issue for years, affecting online security, causing harm to users and third parties and undermining trust in the Internet'. It also presents some recommendations after hearing international, national and EU stakeholders.

Big Ideas 2022

O relatório anual da firma de investimentos ARK revela um conjunto de domínios em que se esperam alguns desenvolvimentos futuros. Em praticamente todos eles, a cibersegurança será uma componente essencial. Leitura a acompanhar com as conclusões e recomendações deste "Study on the need of Cybersecurity requirements for ICT products".

ARK Investments annual report shows a number of areas in which future developments are expected. In virtually all of them, cybersecurity will be an essential component. Follow-up reading with the conclusions and recommendations of this 'Study on the need of Cybersecurity requirements for ICT products'.

Directora | Director
Inês Esteves

Edição | Editor
Pedro Fonseca

Design gráfico | Graphic design
Sara Dias

Tradução | Translation
Sara Pereira

Foto | Photo
Mingwei Lim/Unsplash

Publicação trimestral | Quarterly publication
Abril 2022 | April 2022

Co-financed by the Connecting Europe Facility of the European Union