Segurança e Resiliência do DNS -29 de outubro de 2024

Claire C. van Zwieten - Internet Society Foundation: Então, sejam todos bem-vindos. Ótimo, então vamos lá. Bem-vindos a todos. Obrigado por se juntarem a nós hoje para este webinar muito importante sobre segurança e resiliência do DNS. Este evento é co-organizado pela ICANN e pela Internet Society, e todos os nossos palestrantes são ex-alunos de ambas as organizações.

Aposto que muitos de nós conhecem o DNS, Sistema de Nomes de Domínio, que serve como a espinha dorsal da Internet, conectando usuários em todo o mundo a serviços de informação, mas eles são alvos de ameaças cibernéticas. É importante que, como comunidade, entendamos quais são as ameaças à segurança do DNS e como podemos ser resilientes, e, acima de tudo, o papel das organizações multissetoriais em garantir que possamos combater as ameaças sempre que elas surgirem.

Antes de começarmos, gostaria de convidar o Jadiel, que falará um pouco sobre o nosso programa Pulse. Então, Jadiel, se você quiser vir e começar.

Jadiel ADEFOULOU - Internet Society: Ok, ótimo. Eu sou Jadiel Adefoulou, sou consultor de engenharia de dados para a Internet Society. É um prazer para mim estar aqui e falar sobre a plataforma Pulse.

Então, primeiramente, o que é o Internet Society Pulse? É importante saber que o Internet Society Pulse consolida dados de medição da Internet de terceiros confiáveis de várias fontes em uma única plataforma. Usamos os dados apresentados para examinar as tendências da Internet e adaptar os dados às necessidades dos usuários.

Utilizamos os dados apresentados para examinar as tendências da Internet e contar histórias baseadas em dados, para que os formuladores de políticas, analistas de pesquisa,

operadores de rede, grupos da sociedade civil e outros possam entender melhor a viabilidade, evolução e resiliência da Internet.

Então, no Pulse, monitoramos interrupções da Internet, estimamos o impacto econômico de uma interrupção usando o Calculador de Perda Líquida do Pulse, medimos a resiliência da Internet, acompanhamos o número de pontos de troca de Internet ao redor do mundo,

e oferecemos um relatório por país, uma maneira fácil de obter uma visão geral do estado da Internet em cada país ISO do mundo.

Então, e o DNS?

Especificamente? Dois em cada três domínios de códigos de países são seguros com DNSSEC. Um em cada três usuários da Internet está protegido por um resolvedor que valida DNSSEC. Outra estatística sobre DNSSEC: você pode dizer que alguns países, como a Suécia, têm um incentivo para provedores adotarem DNSSEC. Consequentemente, vemos um nível relativamente alto de cobertura de segurança de nomes.

A maioria dos domínios da Internet tem um nível muito baixo de adoção do DNSSEC. Por exemplo, o domínio .com tem apenas 4% de assinaturas.

Claire C. van Zwieten - Internet Society Foundation: Obrigado, Jadier. Muito obrigado por nos educar sobre o programa Pulse e sobre o DNSSEC.

Agora, gostaria de convidar nossos painelistas para este webinar. Temos Jackie Akello, Kanaan Ngutu, Lia Solis e Marko Paloski. Obrigado a todos por estarem conosco hoje. Kanaan, sei que é muito cedo para você. Provavelmente são cerca de 3 da manhã em Kiribati, então muito obrigado.

Gostaria de dar a todos os nossos palestrantes a oportunidade de se apresentarem e compartilharem um pouco sobre sua opinião sobre o estado atual do DNS. Lia, você gostaria de começar?

Lia Solis Montaño: Bom dia a todos. Eu sou Lia Solis. Minha formação é técnica. Trabalho em um ISP há muitos anos. Trabalho com DNS para ISP, em resolvedores de DNS. Adoro esse ambiente de DNS e sou engenheira de sistemas. Obrigada.

Claire C. van Zwieten - Internet Society Foundation: Incrível. Obrigado por compartilhar.

Marko, você gostaria de ser o próximo?

Marko Paloski - Netcetera: Sim. Obrigado. Olá a todos. Eu sou Marko Paloski, venho de Skopje, na Macedônia, e trabalho como engenheiro de sistemas em uma empresa privada, mais na parte de infraestrutura, mas além disso, também sou coordenador do capítulo do Fórum de Governança da Internet da Macedônia do Norte, e participei da bolsa de estudos da Internet Society, e também da ICANN Next Generation And fellowship.

Então, eu diria que isso é mais ou menos para mim. Como uma pessoa de tecnologia, estou mais interessado em cibersegurança, privacidade, segurança online, fragmentação da Internet e regulação de plataformas, esses tipos de tópicos. Mas sim, muito obrigado.

Claire C. van Zwieten - Internet Society Foundation: Obrigado, e adoro que o Marko mais uma vez destaque que todos neste painel são ex-alunos da ISOC e da ICANN. Todos são especialistas nesta área e participaram das melhores bolsas de estudo do setor para provar isso.

Então, Jackie, você pode se apresentar e compartilhar sua opinião sobre o estado atual do DNS?

Jackie Akello - Research ICT Africa: Muito obrigado por isso, Claire.

Oi, pessoal. É um prazer estar com vocês nesta chamada, são seis horas em Nairóbi. Já é quase noite por aqui, ou melhor, já é noite.

Sou um Pesquisador de IA na Research ICT Africa, e meu trabalho gira fortemente em torno de IA e governança de dados. Principalmente, faço pesquisas e análises de políticas sobre questões emergentes de IA e governança de dados.

Além disso, tive o privilégio de ser um bolsista da ISOC, fazendo parte da turma de 2020, e pude participar do IGF através dessa bolsa. Também fui bolsista da ICANN várias vezes, incluindo as reuniões ICANN 73 e ICANN 77.

É um prazer estar com todos vocês nesta chamada, e estou ansioso para ouvir suas opiniões e até mesmo começar a conversa sobre a segurança do DNS. Obrigado.

Claire C. van Zwieten - Internet Society Foundation: Obrigado.

Kanaan, você gostaria de se apresentar e compartilhar um pouco sobre o que está fazendo profissionalmente e sua opinião sobre o estado atual do DNS?

Kanaan Ngutu - Digital Kiribati: Sim, absolutamente.

Primeiramente, foi, e é, um prazer para mim participar desta conversa, apesar de ser muito cedo pela manhã deste lado do mundo.

Meu nome é Kanaan, e como você já mencionou antes, todos nós fazemos parte dos ex-alunos da ICANN e ISOC. Participei de duas reuniões da ICANN e também de duas reuniões da ISOC no passado, e atualmente trabalho em várias áreas. Faço consultoria na área de TIC, também trabalho com a ITU em projetos de ilhas inteligentes em Kiribati, mas ao mesmo tempo estou liderando uma ONG chamada Digital Kiribati, que trabalha para promover a segurança cibernética e a alfabetização digital na comunidade aqui em Kiribati.

Claire C. van Zwieten - Internet Society Foundation: Obrigado.

Acho que algo que quero compartilhar é que o que torna este grupo muito especial é que todos vêm de grupos de interesse muito variados. Todos têm opiniões e visões muito diferentes sobre a segurança e resiliência do DNS.

Eu adoraria começar com você, Lia. Qual é o papel da segurança e resiliência do DNS no trabalho que você faz, e qual é a sua opinião sobre onde estamos nesse espaço em outubro de 2024?

Lia Solis Montaño: Certo. O DNS é um serviço com uma função definida, que é traduzir nomes de domínio em endereços IP. Com esses endereços, os pacotes podem seguir o melhor caminho definido pelo equipamento de roteamento. Você consegue imaginar um mundo onde todos os usuários têm que memorizar endereços IP?

Precisamente, um dos fatores que promoveu o crescimento da Internet em geral é a facilidade de uso, graças ao DNS. O DNS é um serviço crítico para a acessibilidade da Internet, portanto merece atenção especial em contextos de segurança. Para citar alguns, podemos mencionar o envenenamento de consultas, onde as origens das respostas DNS são alteradas e contêm informações falsas para manipular o destino dos pacotes.

A comunidade técnica tem trabalhado arduamente para evitar essas ameaças.

Claire C. van Zwieten - Internet Society Foundation: Obrigado. E você mencionou a comunidade técnica, e isso me faz querer falar com o Marko. Com base no seu trabalho e no que você faz, como você acha que o DNS mudou talvez nos últimos 10 anos?

Como os riscos de segurança e nossos modelos de resiliência e DNS mudaram?

Marko Paloski - Netcetera: Sim. Obrigado pela pergunta. Eu diria que até mesmo nos últimos dois ou três anos, o que mudou, não apenas em 10 anos, porque no mundo de hoje, a cada ano temos muitos novos desafios e oportunidades e novas tecnologias, novas versões, tudo está mudando e indo em uma direção melhor.

Mas sim, eu concordo, é uma boa pergunta. Nós também, como pessoas, estamos um pouco mais conscientes das coisas, porque usamos a tecnologia todos os dias e cada vez mais, mas por outro lado, devido ao uso de algumas de nossas habilidades, ainda estamos carentes de conhecimento ou talvez não de conhecimento, mas talvez de foco nas coisas.

É por isso que, nos últimos anos, acho que temos cada vez mais ameaças cibernéticas, especialmente no lado do DNS. Diferentes tipos de ataques. Isso está aumentando porque agora somos mais dependentes da tecnologia que temos em cada dispositivo. Até mesmo nos carros, temos tecnologia, sistema e um computador, o que nos torna mais alvos de ataques. Há 10 anos, talvez os alvos fossem as instituições, talvez as empresas, os governos. Agora, eles ainda são alvos, mas agora também o usuário final é muito visado.

É um momento desafiador.

Estamos mais conscientes agora, porque há muitas iniciativas. Claro, algumas vêm da Internet Society. A ICANN também está fazendo muito trabalho nisso para a segurança do DNS, mas ainda acho que estamos longe de estarmos sempre seguros. O DNS é um sistema crítico, mas eu diria que é um dos mais visados, porque, como a Lia mencionou, é uma das coisas centrais da Internet.

Você não pode imaginar a Internet sem o DNS, especialmente a segurança do DNS, que hoje é padrão. No passado, talvez você não precisasse de extensões de segurança do DNS ou algo do tipo, mas hoje você não pode ficar sem isso.

Então, eu diria que com o avanço da tecnologia, também avançam os ataques e as vulnerabilidades. Agora temos inteligência artificial, você pode pedir ao GPT para escrever ou fornecer alguma vulnerabilidade de um site, ou talvez criar uma ferramenta para você.

Por um lado, é bom porque você pode ver e testar mais os sistemas, pois pode ver como as máquinas estão funcionando, mas também dá muito poder a algumas pessoas com más intenções. Talvez elas não tenham más intenções, mas quando você tem a ferramenta, você pode tentar usá-la.

Então, sim, é desafiador, mas nosso trabalho é muito crucial, tanto para os técnicos quanto para os formuladores de políticas e todas as outras pessoas, porque o tema é importante. O multissetorialismo aqui é uma das coisas cruciais, porque acho que a Internet é baseada no multissetorialismo e deve continuar assim. Cada parte interessada, seu trabalho é muito crucial, especialmente nestes tempos que estamos enfrentando.

Não sei se respondi diretamente a pergunta inteira ou se fui um pouco além, mas queria tentar dar alguma resposta.

Claire C. van Zwieten - Internet Society Foundation: Você definitivamente levantou um ponto muito importante, que é que quanto mais nossas vidas se tornam digitais, elas se tornam igualmente vulneráveis, porque, como você disse, hoje em dia temos um computador em nossos carros e em tudo mais, então faz sentido que, à medida que nosso uso dessas coisas aumenta, nossa vulnerabilidade também aumenta.

E Kanaan, quero falar com você, porque sei que você trabalha muito com a comunidade na sua área. E, como você também lida bastante com segurança cibernética, estou curioso para saber como você tem conversado com as pessoas da sua comunidade sobre esse tema, e se conseguiu encontrar maneiras de preencher a lacuna técnica para pessoas que obviamente conhecem a Internet, mas não necessariamente sabem sobre as infraestruturas que a mantêm tão segura como é.

Como Marko disse, você não pode ter a Internet sem DNS, mas muitas pessoas não sabem disso, na verdade. Então, ao falar com sua comunidade sobre cibersegurança, como você consegue incluir isso na conversa?

Kanaan Ngutu - Digital Kiribati: Minha discussão sobre este tópico giraria em torno da experiência do Pacífico, vinda do Pacífico Sul.

Conhecemos o DNS como ele é e seu papel em toda a infraestrutura da Internet. É um dos elementos cruciais que precisa ser protegido. Sabemos da importância do DNS, pois ele pode determinar o destino da Internet, e para que os recursos sejam acessíveis na Internet, precisamos desse elemento crítico.

Isso é especialmente verdadeiro no contexto das Ilhas do Pacífico. Temos operado do outro lado do mundo, praticamente desconhecidos para a maioria das pessoas no mundo ocidental, mas totalmente dependentes da Internet, e temos partes interessadas envolvidas na formação da Internet como ela é, e no seu desenvolvimento futuro.

Mas, infelizmente, a maioria das pessoas, especialmente aquelas que deveriam ter um papel na manutenção desse recurso, não necessariamente conhecem esse elemento crítico da Internet, certo? Acho que isso destaca a importância de envolver cada vez

mais pessoas, e acredito que engajar as pessoas começaria com a construção da capacidade dessas pessoas.

Como você mencionou corretamente, eu aprendi muitas coisas, e uma delas é que a maioria das pessoas não tem conhecimento sobre DNS. Elas nem sabem quais são as vulnerabilidades, quais são as ameaças de segurança que comprometem as operações de DNS no Pacífico, e quando você fala sobre cibersegurança, as pessoas na minha comunidade tendem a ser muito vulneráveis em comparação com pessoas de outras partes do mundo. Em parte porque a Internet é relativamente nova em nosso horizonte quando comparamos com algumas pessoas que estão talvez nos EUA ou na Europa.

Você pode imaginar usar a Internet pela primeira vez, com seus vastos recursos. As pessoas acreditam que a Internet é uma coisa realmente boa, isso é um fato, mas elas não sabem quais são as ameaças dentro da Internet. Existem coisas como abuso infantil online, golpes e ataques que são realizados nas redes e também em indivíduos.

Então, essas são as coisas sobre as quais as pessoas no Pacífico não têm conhecimento, o que as torna ainda mais vulneráveis a esse tipo de ataque. É o mesmo quando você considera o DNSSEC, e acredito que as pessoas perceberiam quando fossem atacadas, é nesse momento que elas perceberiam a necessidade de aprimorar suas habilidades e se manterem informadas e engajadas nessa área tão importante.

Claire C. van Zwieten - Internet Society Foundation: Obrigado pela resposta. Adorei o que você disse e acho que você tem um ótimo ponto quando fala sobre capacidade, que as pessoas não sabem o que não sabem, e se tivessem os recursos para aprender as melhores maneiras de se proteger, seria mais fácil para elas.

Felizmente, agora em 2024, temos a IA, que está proporcionando muitas novas oportunidades para desenvolver as capacidades das pessoas em diversos âmbitos. Gostaria de passar para a Jackie e ver se ela poderia nos trazer alguma informação ou insight sobre o papel da IA no DNS, e se as pessoas estão usando inteligência artificial para ajudar a se educar ou a se manter mais seguras.

Jackie Akello - Research ICT Africa: Muito obrigado por essa pergunta, Claire. Meus colegas compartilharam insights muito importantes sobre a segurança do DNS e também sobre o estado atual do DNS no mundo, então vou compartilhar algumas percepções sobre o papel da IA, especialmente na manutenção do sistema DNS.

O que você viu recentemente, especialmente nos últimos anos, é que a IA realmente cresceu e agora temos IA generativa e o ChatGPT. O papel que vejo a IA desempenhar, particularmente no contexto africano e também para as pessoas nas bases e nos sistemas educacionais, é que agora ela educa as pessoas sobre os sistemas DNS. As pessoas passam a ver quão crucial é o sistema DNS, como ele funciona como uma infraestrutura e também a entender o papel crucial que ele desempenha.

Outra coisa é que a IA também, apenas através das ferramentas educacionais, expõe as pessoas aos danos que podem ser causados aos sistemas DNS. As pessoas sabem que, embora a infraestrutura DNS seja uma infraestrutura crítica, apenas ao se comunicarem e até mesmo ao se conectarem umas com as outras, existem danos ao usar outros sistemas, e elas também são equipadas com informações sobre como podem se proteger.

Outra coisa é que a IA também está sendo usada para causar insegurança no sistema DNS, então questões relacionadas à cibersegurança, danos e até ataques são criadas apenas pelo uso de sistemas de IA. Este é um risco crucial que realmente precisa ser abordado em termos de análise dos sistemas DNS e da IA.

A IA também desempenha um papel crucial na formulação de políticas em torno dos sistemas DNS, pois envolve partes interessadas essenciais no desenvolvimento desses sistemas de IA, além de compartilhar conhecimentos sobre como alguns desses danos podem ser prevenidos e mitigados.

Portanto, a IA tem um papel crucial na segurança do DNA e também no avanço da formulação de políticas em torno do sistema de DNA.

Claire C. van Zwieten - Internet Society Foundation: Obrigado. Essa foi uma ótima resposta. Acho que é realmente importante que as pessoas comuns, o caixa do supermercado, sua mãe, seu pai, todos saibam como se proteger e as melhores práticas para a segurança do DNS.

Se vocês pudessem dizer, eu adoraria que cada um dos nossos palestrantes respondesse a esta pergunta: se vocês pudessem dar um conselho prático para as pessoas que querem se proteger e garantir que estão mantendo um sistema resiliente com uma segurança robusta de DNS, o que vocês sugeririam?

E podemos começar com a Lia.

Lia Solis Montaño: Podemos falar sobre as melhores práticas, por exemplo. É importante entender a recomendação para a implantação e operação do serviço de resolução de nomes, mas também estar aberto ao fato de que essas recomendações são dinâmicas, baseadas em cada ameaça identificada na Internet.

Podemos citar algumas melhores práticas, por exemplo, ter DNS autoritativo e DNS de resolução em diferentes ferramentas de infraestrutura, garantir a redundância dos servidores DNS da maneira mais transparente possível para o usuário. Uma delas pode ser o uso de nuvens anycast, que nos permite ter o servidor com o mesmo IP identificando diferentes localizações geográficas.

Além disso, realize um bom dimensionamento da infraestrutura com base no tráfego gerado pelos usuários da rede. Essas medidas restringem especificamente consultas recursivas aos endereços IP dos usuários-alvo, garantindo a veracidade das respostas às consultas carregadas no DNSSEC?

O melhor guia para o DNS KIND é consultar as plataformas de aprendizado fornecidas pela ICANN e também pela Internet Society sobre esses tópicos.

Neste ponto, gostaria de acrescentar que todas as partes devem entender que o DNS não é uma ferramenta para bloqueio. Este é um tópico muito amplo que pode ser abordado em outro webinar, mas considero importante mencioná-lo para orientar o pensamento dos múltiplos atores.

Obrigado.

Claire C. van Zwieten - Internet Society Foundation: Obrigado, e obrigado por compartilhar que tanto a ICANN quanto a Internet Society têm ótimos recursos sobre segurança DNS, e os melhores guias que você pode obter para se proteger. Obrigado por compartilhar isso, acho que é importante para o público saber.

E então, Marko, eu adoraria ouvir sua resposta também sobre quais são as melhores práticas em segurança de DNS e o que o cidadão comum pode fazer para se proteger.

Marko Paloski - Netcetera: Sim. Depende do sistema, é claro, mas existem muitas boas práticas. Como você mencionou, há muitas da Internet Society e da ICANN que ajudam a escolher ou encontrar o que é relevante. Porque, nem sempre a organização, a empresa ou o indivíduo tem o conhecimento ou o recurso, não precisa ser apenas dinheiro, mas pessoas com conhecimento que sabem o que fazer.

Do ponto de vista técnico, a implementação de DNS Security, DNS seguro, há 10 anos, talvez fosse uma característica vantajosa ou algo assim, de alto nível, mas hoje acho que é uma das coisas básicas que você deve implementar de alguma forma, se quiser ter um DNS seguro ou um sistema seguro, porque o DNS é uma das coisas principais que, se o hacker conseguir acessar, sua empresa ou organização estará vulnerável e aberta a ataques, aberta a um hacker.

Há muitas outras coisas que algumas talvez existissem no passado, outras talvez não, mas durante essa ascensão da nova tecnologia, uso diário, muitas delas são especificadas e talvez avançadas, então eu acrescentaria mais sobre monitorar e registrar o tráfego DNS. Especialmente com a IA hoje em dia, há muitos sistemas que podem ver o comportamento da rede, ver as solicitações, esse tipo de coisa, mas também verificar manualmente e observar porque, à medida que as máquinas de defesa ou a inteligência artificial avançam, também os atacantes avançam. Ambos os

lados têm seus pontos positivos e negativos, e sempre, quando um lado avança, o outro também avançará depois de algum tempo.

Existem muitas listas negras aplicando limitação de taxa, quantas solicitações em um certo tempo podem ser enviadas ou recebidas, ou talvez processadas. Dependendo dos sistemas, podemos ver que, especialmente quando ocorrem ataques DDoS, muitas empresas e sites estão fazendo limitação no período de tempo, quantas solicitações você pode fazer, o que eu acho muito inteligente e uma coisa boa de implementar, dependendo do sistema e do propósito.

Então, ter servidores DNS redundantes, ataques DDoS, a ideia toda é desligar ou tirar a capacidade do servidor, então se você tiver redundância, talvez seja uma infraestrutura melhor, ou resiliente.

Sempre, também para o usuário final, ter todas as atualizações, ou a aplicação atualizada, o sistema operacional, o BIOS, a rede, os switches, depende do tamanho e do que é a empresa, mas tudo deve estar atualizado. Isso é uma coisa fácil e pequena, mas muitas vezes as pessoas esquecem de fazer essas coisas. Especialmente, apenas para nossos telefones quando não os atualizamos ou esquecemos de atualizar a aplicação, mas se você olhar na história dos ataques, ou o que acontece ou alguns que ganharam publicidade, podemos ver que muitas das coisas eram, algum software não estava atualizado, algo era uma versão mais antiga, e essas coisas.

Claro, nem sempre é possível estar atualizado, devido a certas limitações ou ao aplicativo que você está usando, mas ainda assim é algo crucial. Se você perceber que algum software não foi atualizado, eu ainda atribuiria isso a uma pessoa, um erro, porque alguém precisa atualizar, não é como se a IA fizesse isso automaticamente. Então, a maioria dos ataques que ocorreram são erros dos funcionários, ou das pessoas que estão mantendo ou trabalhando nos servidores.

Há mais algumas coisas. Lista negra, também filtragem de DNS. Isso também acontece de tempos em tempos, o que às vezes é para um bom uso, mas às vezes para um mau uso, onde alguns países ou regiões são limitados de acessar ou enviar. No bom sentido, digo que você pode limitar se pedidos maliciosos ou específicos estão chegando, mas em tempos ruins, como alguém mencionou dos painelistas, o DNS não é uma maneira de bloquear a Internet ou de bloquear o acesso, mas de dar acesso. Podemos ver em alguns casos que às vezes o DNS é usado por estados nacionais para bloqueio.

E, sim, sempre a lista de controle de acesso, e talvez limitar zonas para transferência. Isso é mais especificamente para partes técnicas, onde a transferência de endereços IP, ou onde você pode pegar um novo ou algo assim.

Esses são cinco, seis, sete que mencionei, mas esses são os básicos. Existem muitos mais complicados, e eu sei que no trabalho também temos algum tipo de software, que

eu não sabia que esse tipo de restrição sofisticada podia ser aplicada, mas faz sentido depois que você vê o tipo de ataques que estão surgindo.

Então, você sempre tenta se proteger de qualquer tipo de ameaça, mesmo que não seja uma ameaça, apenas para estar protegido, porque às vezes, talvez amanhã, isso se torne uma ameaça, mesmo que hoje não seja, então eu daria essas como melhores práticas.

Claire C. van Zwieten - Internet Society Foundation: Eu quero rapidamente, enquanto temos você aqui, Marko, compartilhar uma pergunta que foi feita no chat pela Sana. Ela diz: Obrigada a todos por compartilharem seu conhecimento importante conosco. Você mencionou a importância da colaboração multissetorial na segurança do DNS. Por favor, compartilhe seus pensamentos sobre etapas práticas específicas que diferentes partes interessadas, como empresas privadas, agências governamentais e especialistas técnicos, podem tomar para melhorar a colaboração na segurança de um sistema DNS. Existem áreas específicas onde o trabalho em equipe pode ser aprimorado tanto em ameaças existentes quanto emergentes?

Na verdade, gostaria que o maior número possível de nossos palestrantes, que se sentirem à vontade, compartilhassem sua opinião sobre isso, porque é uma ótima pergunta. Então, Marko, como a pergunta foi direcionada a você, gostaria de responder?

Marko Paloski - Netcetera: Posso dizer que é uma pergunta muito boa porque, às vezes, especialmente na correlação de DNS, quando você pergunta sobre empresas, porque também trabalho em uma empresa privada, não é muito compreendido, porque se entendessem os benefícios que esse multissetorialismo pode trazer, acho que todos o desejariam. Claro, às vezes é uma falta de conhecimento de como isso funciona.

Acho que o multissetorialismo é uma abordagem muito boa, especialmente neste tópico, porque a Internet e a governança da Internet são baseadas nisso, especialmente quando, como você mencionou, empresas privadas, agências governamentais, especialistas técnicos, nem sempre essas instituições corporativas têm os recursos e o conhecimento.

Talvez algumas instituições tenham um conhecimento muito bom em cibersegurança, outras, talvez tenham o software, mas não têm os recursos, e é muito crucial haver cooperação e comunicação entre elas. Além disso, eu venho de um país pequeno, a Macedônia. Temos um CERT, mas é muito pequeno e não está tão preparado para grandes ataques ou algo assim.

Frequentemente, o que vejo é que às vezes as empresas ajudam o governo ou alguma organização a mitigar esse tipo de ataque. Infelizmente, não existe uma plataforma

global onde todos os países ou empresas possam se unir, mas há muitas iniciativas em andamento que indivíduos, governos ou empresas privadas podem participar.

É muito bom mencionar, aqui, porque fazemos parte deste webinar, posso destacar que há algumas organizações que estão fazendo diferentes tipos de coisas sobre multissetorialismo, para melhores práticas e também definição de padrões. A ICANN está fazendo muito, assim como o Internet Engineering Task Force, que está desenvolvendo os padrões, eles estão desenvolvendo melhores práticas, você pode encontrar no site.

A Internet Society também é uma delas, junto com a ICANN na defesa de políticas e conscientização. Há muitas iniciativas da Internet Society que as pessoas podem participar, e também há uma rede de especialistas onde você pode compartilhar ou perguntar nos fóruns. Havia o DnS Abuse Institute, mas agora acho que mudaram o nome, é mais sobre resposta a incidentes e mitigação e colaboração nessas coisas.

Então, existem muitas plataformas ou talvez fóruns que podem ser úteis para empresas, organizações e coisas desse tipo. Para organizações, eu não diria tanto, mas para empresas e governos, vejo a falta de benefícios em participar ou usar tanto.

A empresa, às vezes diz não, não podemos pagar alguém, podemos resolver isso, não queremos colaborar, ou às vezes a empresa não quer compartilhar o que aconteceu, nem publicamente.

E o governo, depende do governo, é claro, às vezes eles querem resolver sozinhos. Tivemos um caso em nosso país onde houve um ataque ao servidor, mas no final descobriu-se que foram eles que organizaram isso, para roubar ou lavar dinheiro.

Então, às vezes é um problema, mas é algo muito crucial, porque se todos cooperarem, será muito mais fácil mitigar ataques e também estar mais seguro.

Claire C. van Zwieten - Internet Society Foundation: Concordo com você, sobre o que disse quando os governos tentam fazer isso internamente. Claro, eles provavelmente têm uma variedade de diferentes habilidades dentro do governo, mas realmente nada formativo, nenhuma mudança verdadeira e robusta acontece sozinha.

Então, eu realmente gostaria de chamar a Jackie e perguntar a opinião dela sobre a abordagem multissetorial para a segurança e resiliência do DNS, e onde há mais oportunidades de colaboração que provavelmente deveriam ser exploradas.

Jackie Akello - Research ICT Africa: Muito obrigado, Claire.

O multissetorialismo desempenha um papel muito importante na segurança e também na resiliência dos sistemas de nomes de domínio. Essas organizações reúnem diversos

stakeholders, incluindo governos, entidades privadas, organizações da sociedade e também especialistas técnicos.

Quando essas organizações se reúnem, elas garantem que diversas perspectivas e interesses que moldam as políticas, padrões técnicos e estruturas sejam compartilhados, permitindo a governança da Internet de uma maneira muito significativa e frutífera, o que fortalece a segurança do nosso DNS.

A importância reside em manter uma Internet aberta, inclusiva e resiliente que reflita as necessidades de todos os usuários, ao mesmo tempo em que aborda as complexidades de uma rede global interconectada.

Acredito que o modelo multissetorial desempenha um papel fundamental na segurança do DNS devido aos valores únicos que adiciona na formulação de políticas. Por exemplo, ele permite inclusão e representação. O que acontece é que as organizações multissetoriais realmente reúnem diferentes vozes de governos, do setor privado e de entidades técnicas. No final das contas, a inclusão garante que a governança da Internet reflita as diversas necessidades e prioridades, em vez de favorecer apenas um grupo específico no ecossistema do DNS.

Outra vantagem do multissetorialismo é que ele permite transparência e responsabilidade. Decisões sobre DNS tomadas através de processos multissetoriais são geralmente mais transparentes e responsáveis quando várias entidades estão envolvidas na formulação dessas decisões.

Organizações como o IGF criam fóruns abertos onde políticas e práticas podem ser debatidas. Elas podem ser discutidas e revisadas por pessoas com diferentes especializações nos sistemas DNS. O que acontece no final do dia é que as pessoas compartilham as melhores práticas que podem governar os sistemas DNS da melhor maneira possível no futuro.

Outra vantagem do multissetorialismo é a inovação e a capacidade de resposta. Como todos sabemos, a tecnologia avança em um ritmo muito rápido. Então, quando você envolve pessoas de diferentes setores, como organizações da sociedade civil, o que acontece é que as pessoas compartilham suas experiências e até mesmo sua expertise nas tecnologias atuais que temos, garantindo que as leis vigentes também estejam em sintonia com o avanço das tecnologias.

As pessoas podem compartilhar o que está acontecendo no espaço tecnológico, quais novas tecnologias estão sendo lançadas e quais considerações e medidas políticas precisam ser implementadas para garantir a segurança do DNS.

Outra vantagem disso é que, no final das contas, todos os interesses foram considerados, garantindo um equilíbrio em termos dos interesses apresentados nos

debates sobre questões de DNS. Temos diferentes setores, temos a sociedade civil, temos o governo e os formuladores de políticas. Quando todos se reúnem à mesa, discutem e concordam sobre questões-chave, o que obtemos no final do dia é que seus interesses estão equilibrados e todos foram atendidos em relação à opinião que têm sobre a segurança do DNS.

Uma última coisa que posso dizer sobre o multissetorialismo é que ele também constrói confiança e legitimidade no sistema, porque todas as vozes foram consideradas. Todos puderam compartilhar suas opiniões em relação à formulação de políticas sobre o DNS e até mesmo à segurança do DNS.

O que acontece é que, quaisquer que sejam as regras e políticas aprovadas no final do dia, elas podem ser consideradas legítimas porque a voz de todos foi considerada no desenvolvimento dessas políticas, e a opinião de todos também foi levada em conta.

Então, o que obtemos no final do dia é que isso garante legitimidade em comparação a ter apenas um grupo isolado tomando decisões sobre questões de DNS e também aprovando políticas. Quando isso acontece, há muita desconfiança, e as pessoas não consideram essas políticas e decisões como legítimas.

Então, em resumo, posso dizer que essas são algumas das vantagens que temos com o multissetorialismo no sistema.

Obrigado,

Claire C. van Zwieten - Internet Society Foundation: e obrigado por mencionar o importante aspecto da confiança por design. Quando desenvolvemos políticas e sistemas com segurança e confiança em mente, isso tem um efeito cascata, através dos usuários, através da comunidade que utiliza esses sistemas. Então, obrigado por trazer isso à tona e também por destacar o lado das políticas.

Essa é uma ótima deixa para chamar o Kanaan novamente. Ele é um consultor de políticas, e eu adoraria ouvir sobre sua experiência na criação de políticas e consultoria em políticas como DNS, e que tipo de desafios e também oportunidades você encontrou nesse processo.

Kanaan Ngutu - Digital Kiribati: Novamente, falando das Ilhas do Pacífico, quero falar dentro do meu próprio contexto, e acho que a experiência é semelhante com o DNS e todas as outras partes da política em outras áreas.

Começou com a necessidade de envolver as partes interessadas, que deveriam estar envolvidas, para entenderem melhor a natureza do trabalho, e isso é para garantir que elas possam contribuir de forma significativa para a discussão e para moldar os

aspectos da política com DNS no Pacífico. Como mencionei antes, poucas pessoas entendem isso.

Eu entendo que existem várias plataformas criadas no cenário internacional que promovem o engajamento nessa área, mas um dos principais desafios que temos em Kiribati e nas Ilhas do Pacífico é que temos um fuso horário muito diferente de outros países.

Então, está claro que precisamos criar nosso próprio espaço, como um subespaço, que incentive os atores locais a se envolverem em um nível pessoal. O que quero dizer com isso é que, em Kiribati, o que fazemos é tentar identificar campeões, campeões que incentivem os artistas a se envolverem e discutirem essas questões. É aqui que o apoio da ICANN e da ISOC na produção de recursos que podemos usar localmente, e podemos traduzir essas coisas, é fundamental para garantir que as pessoas interessadas tenham uma compreensão abrangente, porque é aí que começaremos a construir a capacidade a partir do nível local.

À medida que amadurecem ou se familiarizam com o conhecimento necessário, eles podem levar isso e elevar os engajamentos ao nível regional e, posteriormente, ao nível global ou internacional, no que diz respeito à discussão de questões relacionadas à política.

Acho que é assim que devemos começar no Pacífico, e isso também se aplica a outras partes do mundo que se consideram isoladas de toda a comunidade global. Você precisa começar dentro da sua própria sociedade e envolver as partes interessadas, desenvolvendo suas capacidades, porque a partir daí você pode garantir que, quando quiserem levar seus compromissos para o próximo nível, eles serão mais significativos e eficientes nesse aspecto.

Isso se aplica ao DNS e também a todos os campos onde é necessário desenvolver políticas e adotar um modelo de múltiplas partes interessadas.

Claire C. van Zwieten - Internet Society Foundation: O papel dos campeões na criação de sistemas e políticas robustas que protejam e defendam a Internet é crucial. Um pequeno elogio aqui, algo realmente ótimo sobre a ICANN e a Internet Society, é que podemos ter esses programas pelos quais todos nesta chamada passaram, e através disso, vocês se tornaram campeões por direito próprio, e campeões da Internet.

Seja técnico ou político, ou o que quer que seja, vocês conseguiram levar essas habilidades de volta para suas comunidades e implementá-las para o bem. É importante que continuemos a criar e desenvolver campeões como vocês quatro, para que possam realmente fazer, honestamente, o trabalho pesado de defesa da Internet. São vocês, em suas posições, em seus empregos e em suas vidas, que realmente protegem a Internet e fazem tudo o que precisamos fazer.

Então, muito obrigado a todos por tudo o que fazem, e muito obrigado por tudo o que acrescentaram a esta conversa.

Antes de encerrarmos por causa do tempo, eu adoraria responder às três perguntas que temos na sessão de perguntas e respostas, e começarei com a primeira de Ryan Uddin. Quais vulnerabilidades no DNS o tornam suscetível a ataques de spoofing? Você gostaria de responder a essa, Lia?

Lia Solis Montaño: Certo. Quando precisamos verificar o endereço IP, temos que implementar esses métodos de falsificação em nossa infraestrutura, e o princípio para fazer isso é o DNSSEC.

Claire C. van Zwieten - Internet Society Foundation: Obrigado.

Então temos outra pergunta do Nicolas, que é um dos ex-alunos da Internet Society. Ele diz: Como o framework KinDNS pode ser otimizado para suportar algoritmos criptográficos resistentes a quânticos, que coleção de palavras, uau! e DNSSEC, à medida que os avanços na computação quântica, como o recozimento quântico, ameaçam métodos de criptografia tradicionais como o RSA 2048.

Nicolas, você está testando minha capacidade de falar hoje. Uau!

Então, Marko, você gostaria de responder a essa?

Marko Paloski - Netcetera: Eu tentaria, porque não estou muito envolvido com computação quântica e esse tipo de criptografia, mas sei que Nicolas está bastante, porque no ano passado, no IGF em Kyoto, ele também estava discutindo e fazendo perguntas sobre isso.

Não tenho certeza, mas sei que esse framework KinDNS, que é da ICANN, é toda a ideia que mencionei anteriormente, multissetorialismo e um lugar para melhores práticas, este é um exemplo do que a ICANN está fazendo com esse framework.

Mas, como otimizar os algoritmos criptográficos resistentes a quântica? Essa é uma boa pergunta.

Claire C. van Zwieten - Internet Society Foundation: Você disse isso com tanta facilidade. Você faz parecer tão fácil.

Marko Paloski - Netcetera: Sim, ele está falando como uma conversa normal de café, mas acho que a criptografia, especialmente agora com a computação quântica, ainda estamos longe desse tipo de processamento grande, mas um dia eventualmente chegaremos lá. A computação quântica desempenha um grande papel agora,

especialmente na criptografia para aqueles que são menos seguros, porque será muito mais fácil, com a computação quântica, decifrar ou encontrar a chave de criptografia.

Isso é relativamente novo. Está em fase de pesquisa, há poucos projetos comerciais que estão ativamente fazendo isso, mas eu acho que mais sistemas se tornarão mais avançados e poderá se tornar mais fácil de ser implementado ou otimizado.

Como mencionei, não tenho muita certeza porque não estou tão envolvido com a computação quântica, especialmente com a criptografia usando computação quântica, mas minha ideia é que, com o tempo, os sistemas serão mais avançados, mais fáceis de otimizar ou configurar com ambas as coisas, porque haverá mais espaço para isso.

Não sei se respondi. Conhecendo o Nikolas, sei que não é a resposta completa.

Claire C. van Zwieten - Internet Society Foundation: Então, infelizmente, Jackie precisa sair, mas muito obrigado, Jackie, por todas as suas percepções hoje, e obrigado por emprestar seu excelente conhecimento em DNS e jurídico a esta conversa.

Agora temos outra pergunta: Quais medidas podem ser tomadas para incentivar a adoção generalizada de práticas de segurança?

Eu gostaria de ir para Canaã para essa.

Kanaan Ngutu - Digital Kiribati: A resposta é obviamente que precisamos conscientizar mais as pessoas, especialmente as organizações. Elas precisam estar mais cientes das ameaças e também orientá-las e ensiná-las sobre quais medidas tomar para começar a implementar a segurança em torno da infraestrutura de DNS.

Isso é muito importante para mim, porque, pelo que sei, em muitas organizações com as quais trabalhei, a maioria das pessoas, mesmo no departamento de TI, nem sequer sabe como tomar medidas para proteger sua infraestrutura de DNS, especialmente no contexto específico.

Novamente, a rede deles é tão simples, não há sofisticação, então como podem implementar DNS se não têm uma infraestrutura de rede adequada?

Então, para incentivar as pessoas a adotar e implementar as melhores práticas, precisamos educá-las e mostrar como isso é feito.

Acredito que a partir daí eles podem construir seu conhecimento para o futuro.

Claire C. van Zwieten - Internet Society Foundation: É uma ótima pergunta e uma ótima resposta. Gostaria que a Lia também abordasse essa questão, e acho que essa será a última pergunta que responderemos antes de, infelizmente, encerrarmos o

webinar. Mas Lia, eu adoraria ouvir de você o que podemos fazer para aumentar as taxas de adoção do DNS.

E o-- qual era o outro acrônimo divertido? O KinDNS.

Lia Solis Montaño: KinDNS oferece nosso guia padrão para ter DNS. É com isso que podemos trabalhar inicialmente para aqueles que querem encontrar um guia. Boas práticas são dinâmicas e se ajustam às necessidades do tempo. Certamente podemos fazer contribuições em cada cenário que possa surgir. Lembre-se de que temos comunidades preocupadas com esse uso.

Claire C. van Zwieten - Internet Society Foundation: Muito obrigado. E acho que o que essa pessoa também perguntou é o que podemos fazer para garantir que estamos estabelecendo padrões de segurança adequados para esses tipos de sistemas.

Algum de vocês tem alguma percepção sobre a importância ou a capacidade de definir padrões?

Marko Paloski - Netcetera: Verifique as melhores práticas, veja quais são algumas coisas conhecidas internacionalmente e de organizações como a ICANN ou a Internet Society.

Verifique também com seu país ou comunidade local o que outras instituições ou governos estão fazendo, ou se há alguma lei. Eu não sei sobre isso, mas ainda assim verifique. Mesmo que não haja nada, tente criar algo e veja se é bom. Se não for, então mude.

Essas coisas não são algo que você faz uma vez e é para a vida toda; você precisa revisar e atualizar constantemente porque a tecnologia muda, os ataques mudam, então precisa estar sempre atualizado.

Isso é tudo.

Claire C. van Zwieten - Internet Society Foundation: Incrível. E, com essa nota perfeita, temos que encerrar este webinar. Muito obrigado aos nossos palestrantes. Obrigado por dedicarem seu tempo e sua manhã para compartilhar seu conhecimento e seu tempo conosco.

Obrigado a todo o nosso público. Obrigado por virem. Espero que tenham aprendido um pouco e estou ansioso para vê-los em nosso próximo evento. Vamos compartilhar isso assim que pudermos. Espero que todos tenham um ótimo dia.