Artigo

26-01-2022 - 17:06
20211111STO17184

Parlamento Europeu

Como o PE pretende reforçar a cibersegurança na UE (entrevista)

Entrevista com o relator Bart Groothuis

Os eurodeputados querem proteger melhor os europeus e as empresas das ameaças crescentes na internet. Lê a entrevista com o relator Bart Groothuis.

Esta entrevista foi realizada antes de a diretiva relativa à segurança das redes e dos sistemas de informação (NIS2) ser adotada pelo Parlamento em novembro de 2022.

À medida que as redes e os sistemas de informação se tornam numa característica central do nosso quotidiano, as ameaças à segurança na internet ganham maiores proporções. Tais ameaças podem causar prejuízos financeiros e chegar mesmo a perturbar o abastecimento de

água e energia ou as operações hospitalares.

Uma cibersegurança forte é crucial para proteger os cidadãos, assimilar a transformação digital e aproveitar plenamente os benefícios socioeconómicos e sustentáveis da digitalização.

Sabe por que razão se deve preocupar com a questão da cibersegurança na UE.

O Parlamento Europeu (PE) aprovou a sua posição negocial sobre a revisão da Diretiva relativa à segurança das redes e da informação (Diretiva SRI), a 11 de novembro. O eurodeputado responsável pelo processo explicou-nos as intenções do PE neste âmbito:

Quais são as ameaças mais proeminentes à cibersegurança?

Ransomware é de longe a ameaça mais significativa. Triplicou em todo o mundo em 2020 e este ano vemos a existência de outro pico. Dez anos atrás, *ransomware* visava indivíduos. Um indivíduo tinha de pagar 100€ ou 200€ ao *hacker*.

Hoje em dia, o pagamento médio é de 140 000€. Não só as grandes empresas, mas também as pequenas empresas estão a ser atacadas e têm de pagar porque não podem operar de outra forma.

É também a ameaça mais significativa porque é um instrumento de política externa para os Estados desonestos.

A ENISA define 'ransonware' como:

- Um tipo de malware que infeta sistemas de computador, impedindo a vítima de usar o sistema e os dados armazenados nele. Geralmente, a vítima recebe uma mensagem de chantagem por pop-up, pedindo o pagamento de um resgate para recuperar o acesso.

De que forma a pandemia de ransomware afeta a vida de um cidadão ou empresa?

Vemos o ransomware visar quase tudo o que oferece serviços aos cidadãos. Pode ser um município, um hospital, um fabricante local.

O Parlamento e o Conselho estão a trabalhar em legislação relativa à cibersegurança. O objetivo é proteger melhor essas entidades contra esses *hackers*.

As empresas da UE que prestam serviços essenciais ou importantes terão de tomar medidas de cibersegurança, e os governos precisam de ter capacidade para ajudar estas empresas e partilhar informações com elas e com outros governos.

O que é que Parlamento quer?

O Parlamento quer que a legislação seja ambiciosa. O âmbito de aplicação deve ser amplo, devemos abranger e ajudar entidades que são vitais para o nosso modo de vida. A Europa deve ser um lugar seguro para viver e fazer negócios. E não devemos esperar, precisamos desta nova legislação rapidamente.

Por que é que a rapidez é importante?

Em [matéria de] cibersegurança, devemos ter a certeza de que não somos os mais fracos. As empresas da UE já estão a investir 41% menos do que as empresas nos EUA [neste campo]. E os EUA estão a mobilizar-se rapidamente, Biden está a criar legislação de urgência e não queremos encontrar-nos numa situação em que a Europa se torna mais atraente para *hackers* de *ransomware* em comparação com outras partes do mundo. Os investimentos em segurança cibernética têm de ser feitos agora.

A segunda razão é que existem problemas na comunidade da cibersegurança que precisam ser corrigidos o mais rapidamente possível. Os profissionais de cibersegurança têm geralmente preocupações com o GDPR: podem ou não partilhar dados de cibersegurança? Deve existir uma base jurídica sólida para partilhar dados de cibersegurança de modo a ajudar a prevenir ciberataques.

Que desafios poderá o Parlamento enfrentar nas negociações?

Haverá debate sobre o âmbito, e quais entidades devem ser incluídas. E teremos que discutir o impacto administrativo para as empresas. O Parlamento considera que a legislação deve proteger as empresas, mas também deve ser prática e exequível; o que podemos razoavelmente pedir?

Outra questão é o núcleo da internet, os sistemas de nomes de domínio e da zona raíz. A Comissão Europeia e o Conselho querem incluir esta questão no âmbito de aplicação das regras e regulamentá-la. Oponho-me veementemente a isso, porque a Rússia e a China vão querer fazer o mesmo, e devemos manter o núcleo livre e aberto e manter o nosso modelo de

múltiplas partes interessadas.

Por que razão é importante ter regras comuns de cibersegurança em todos os países da UE?

A base desta legislação é o funcionamento do mercado interno. Não importa se [alguém] negócios na Eslováquia, na Alemanha ou nos Países Baixos, [porque] vai querer ter a certeza de que há um nível comum de requisitos de cibersegurança e que o país em que se encontra tem uma infraestrutura de cibersegurança operacional. Devemos harmonizar as regras e proteger a vida dos nossos cidadãos.

Sobre a Directiva SRI 2: um elevado nível comum de cibersegurança em toda a UE

Comunicado de imprensa após votação na comissão: "Cibersegurança: eurodeputados reforçam requisitos a nível da UE contra ameaças" (28-10-2021, EN)
Estado do procedimento legislativo (EN)
Progresso legislativo: revisão da diretiva SRI (EN)
Briefing do PE (EN)
Página da Comissão Europeia: diretiva SRI (EN)
Agência da União Europeia para a Cibersegurança (ENISA): definição de 'Ransomware' (EN)