RECOMENDAÇÕES

RECOMENDAÇÃO (UE) 2019/553 DA COMISSÃO

de 3 de abril de 2019

sobre a cibersegurança no setor da energia

[notificada com o número C(2019) 2400]

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 292.º,

Considerando o seguinte:

(1) O setor europeu da energia está a atravessar uma importante mudança rumo a uma economia descarbonizada que garanta, simultaneamente, a segurança do aprovisionamento e a competitividade. No âmbito desta transição energética e da concomitante descentralização da produção de energia a partir de fontes renováveis, o progresso tecnológico, o acoplamento de setores e a digitalização estão a transformar a rede elétrica da Europa numa «rede inteligente». Isto acarreta, contudo, novos riscos, dado que a digitalização expõe cada vez mais o sistema energético a ataques informáticos e a incidentes que podem comprometer a segurança do aprovisionamento energético.

(2) A adoção das oito propostas legislativas ([1]) do Pacote «Energias limpas para todos os europeus», que inclui a governação da União da Energia como elemento impulsionador, permite criar um ambiente favorável à transformação digital do setor da energia. Reconhece igualmente a importância da cibersegurança neste setor. Em especial, a reformulação do Regulamento Mercado Interno da Eletricidade ([2]) prevê a adoção de normas técnicas para a eletricidade, como um código de rede relativo às regras setoriais aplicáveis aos aspetos de cibersegurança dos fluxos transfronteiriços de eletricidade, aos requisitos mínimos comuns, ao planeamento, à monitorização, à comunicação de informações e à gestão de crises. O Regulamento Preparação para os Riscos no domínio da Eletricidade ([3]) segue, em geral, a abordagem adotada no Regulamento Segurança do Aprovisionamento de Gás ([4]); salienta a necessidade de avaliar de modo adequado todos os riscos, nomeadamente os relacionados com a cibersegurança, e propõe a adoção de medidas para prevenir e atenuar os riscos identificados.

(3) Quando a Comissão adotou a estratégia da UE para a cibersegurança ([5]), em 2013, considerou prioritário o reforço da ciberrresiliência. Uma das principais consequências da estratégia é a Diretiva Segurança das Redes e da Informação ([6]) (adiante designada por, «Diretiva SRI»), que foi adotada em julho de 2016. A Diretiva SRI, que constituiu o primeiro ato legislativo horizontal da UE no domínio da cibersegurança, reforça o nível global de cibersegurança na UE através do desenvolvimento das capacidades nacionais neste domínio, do aumento da cooperação a nível da UE e da introdução de obrigações de comunicação em matéria de segurança e de incidentes para as empresas referidas como «operadores de serviços essenciais». A comunicação de incidentes é obrigatória nos setores-chave, dos quais o setor da energia.

([1]) Diretiva (UE) 2018/2001do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, relativa à promoção da utilização de energia de fontes renováveis (JO L 328 de 21.12.2018, p. 82); Diretiva (UE) 2018/2002 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que altera a Diretiva 2012/27/UE relativa à eficiência energética (JO L 328 de 21.12.2018, p. 210); Regulamento (UE) 2018/1999 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, relativo à Governação da União da Energia e da Ação Climática, que altera os Regulamentos (CE) n.º 663/2009 e (CE) n.º 715/2009 do Parlamento Europeu e do Conselho, as Diretivas 94/22/CE, 98/70/CE, 2009/31/CE, 2009/73/CE, 2010/31/UE, 2012/27/UE e 2013/30/UE do Parlamento Europeu e do Conselho, as Diretivas 2009/119/CE e (UE) 2015/652 do Conselho, e revoga o Regulamento (UE) n.º 525/2013 do Parlamento Europeu e do Conselho (JO L 328 de 21.12.2018, p. 1); Diretiva (UE) 2018/844 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva 2010/31/UE relativa ao desempenho energético dos edifícios e a Diretiva 2012/27/UE sobre a eficiência energética (JO L 156 de 19.6.2018, p. 75). Na sessão plenária de março de 2019, o Parlamento Europeu confirmou os acordos políticos alcançados com o Conselho sobre as propostas de configuração do mercado da eletricidade (Regulamento Preparação para os Riscos, Regulamento Agência de Cooperação dos Reguladores da Energia — ACER — Diretiva Eletricidade e Regulamento Eletricidade. Prevê-se que a adoção formal pelo Conselho ocorra em abril; a publicação do ato legal no Jornal Oficial terá lugar pouco depois.

([2]) COM(2016) 861 final.

([3]) COM(2016) 862 final.

([4]) Regulamento (UE) 2017/1938 do Parlamento Europeu e do Conselho, de 25 de outubro de 2017, relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga o Regulamento (UE) n.º 994/2010 (JO L 280 de 28.10.2017, p. 1).

([5]) JOIN(2013) 1.

([6]) Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194 de 19.7.2016, p. 1).

(4) Na execução de medidas de preparação no domínio da cibersegurança, as principais partes interessadas, nomeadamente os operadores de serviços essenciais no domínio da energia identificados como tal na Diretiva SRI, devem ter em conta as orientações horizontais emitidas pelo grupo de cooperação SRI criado ao abrigo do artigo 11.º daquela diretiva. Este grupo de cooperação, composto por representantes dos Estados-Membros, da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e da Comissão Europeia, adotou documentos de orientação sobre medidas de segurança e notificação de incidentes. Em junho de 2018, o grupo criou uma vertente de trabalho específica no domínio da energia.

(5) A Comunicação Conjunta sobre cibersegurança ([7]), de 2017, reconhece que importa abordar a nível da União as considerações e exigências específicas de cada setor, nomeadamente no que respeita ao setor da energia. Nos últimos anos, a cibersegurança e as suas possíveis implicações políticas foram objeto de um amplo processo de debate na União. Por conseguinte, existe hoje uma consciência crescente de que cada setor económico enfrenta questões de cibersegurança específicas e, por conseguinte, tem de definir as suas próprias abordagens setoriais no contexto mais vasto das estratégias gerais de cibersegurança.

(6) A partilha de informações e a confiança são elementos fundamentais da cibersegurança. A Comissão pretende reforçar a partilha de informações entre as partes interessadas através da organização de eventos específicos — como, por exemplo, a mesa redonda de alto nível sobre cibersegurança no domínio da energia, organizada em Roma, em março de 2017, e a conferência de alto nível sobre cibersegurança no domínio da energia, organizada em Bruxelas, em outubro de 2018. A Comissão pretende igualmente reforçar a cooperação entre as partes interessadas e as entidades especializadas, como o Centro Europeu de Partilha e Análise de Informação Energética.

(7) O Regulamento relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação («Regulamento Cibersegurança») ([8]) reforça o mandato da ENISA, para que esta possa apoiar melhor os Estados-Membros no combate às ameaças e aos ataques no domínio da cibersegurança. Estabelece também um quadro europeu de cibersegurança para a certificação de produtos, processos e serviços, que será aplicável em toda a União e se reveste de particular interesse para o setor da energia.

(8) A Comissão apresentou uma recomendação ([9]) que aborda os riscos em matéria de cibersegurança da 5.ª geração de tecnologias de rede (5G), fornecendo orientações em domínios como as medidas adequadas de análise e gestão de riscos ao nível nacional, a adoção de uma análise de riscos coordenada a nível Europeu e a definição de um processo para estabelecer um conjunto de melhores medidas comuns de gestão de riscos. Quando estiverem operacionais, as redes 5G tornar-se-ão a espinha dorsal de uma vasta gama de serviços essenciais ao funcionamento do mercado interno e de instrumentos sociais e económicos essenciais, como a energia.

(9) A presente recomendação deve fornecer orientações não exaustivas aos Estados-Membros e às partes interessadas, em particular aos operadores de rede e aos fornecedores de tecnologias, para alcançar um nível mais elevado de cibersegurança, atendendo aos requisitos específicos em tempo real identificados para o setor da energia, os efeitos em cascata e a combinação de tecnologias clássicas e de ponta. As referidas orientações visam ajudar as partes interessadas a ter em conta os requisitos específicos do setor da energia na aplicação das normas de cibersegurança internacionalmente reconhecidas ([10]).

(10) A Comissão tenciona rever regularmente a presente recomendação à luz dos progressos realizados em toda a União, após consulta dos Estados-Membros e das partes interessadas. A Comissão prosseguirá os seus esforços para reforçar a cibersegurança no setor da energia, nomeadamente através do grupo de cooperação SRI, que assegura a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros em matéria de cibersegurança,

ADOTOU A PRESENTE RECOMENDAÇÃO:

OBJETO

1. A presente recomendação define as principais questões relacionadas com a cibersegurança no setor da energia, nomeadamente os requisitos em tempo real, os efeitos em cascata e combinação de tecnologias clássicas e de ponta, e identifica as principais ações para a aplicação de medidas pertinentes de preparação em matéria de cibersegurança, no setor da energia.

([7]) JOIN(2017) 450

([8]) O Regulamento Cibersegurança foi adotado pelo Parlamento Europeu em março de 2019. Prevê-se que adoção formal pelo Conselho ocorra em abril; a publicação do ato legal no Jornal Oficial terá lugar pouco depois.

([9]) C(2019) 2335

([10]) As organizações de normalização internacionais publicaram vários requisitos em matéria de cibersegurança (ISO/IEC 27000: tecnologias da informação) e normas de gestão dos riscos (ISO/IEC31000: implementação da gestão dos riscos). Em outubro de 2017, foi adotada, no âmbito da série ISO/IEC 27000, uma norma específica para o setor da energia (ISO/IEC 27019: controlos de segurança da informação para os serviços do setor da energia).

2. Ao aplicar a presente recomendação, os Estados-Membros devem incentivar as partes interessadas a adquirirem competências e conhecimentos relacionados com a cibersegurança no setor da energia. Sempre que isso se justifique, os Estados-Membros devem também incluir estas considerações no seu quadro nacional de cibersegurança, nomeadamente através de estratégias, leis, regulamentos e outras disposições administrativas.

REQUISITOS EM TEMPO REAL DAS COMPONENTES DA INFRAESTRUTURA ENERGÉTICA

3. Os Estados-Membros devem assegurar que as partes interessadas, nomeadamente os operadores de redes de energia, os fornecedores de tecnologias e, em especial, os operadores de serviços essenciais identificados na Diretiva SRI, aplicam as medidas de preparação que se impõem em matéria de cibersegurança, relacionadas com os requisitos em tempo real no setor da energia. Alguns elementos do sistema energético têm de funcionar em tempo real, ou seja, reagir a comandos em poucos milissegundos, o que torna difícil ou mesmo impossível aplicar medidas de cibersegurança, por falta de tempo.

4. Em especial, os operadores de redes de energia devem:

   a) Aplicar, sempre que adequado, as normas de segurança mais recentes nas novas instalações e ponderar a adoção de medidas de segurança física complementares no caso das instalações obsoletas que não possam ser suficientemente protegidas por mecanismos de cibersegurança;

   b) Aplicar as normas internacionais em matéria de cibersegurança, bem como as normas técnicas específicas para uma comunicação segura e em tempo real, logo que os respetivos produtos estejam disponíveis no comércio;

   c) Ponderar a adoção de restrições em tempo real no conceito global de segurança dos ativos, especialmente no que se refere à classificação destes;

   d) Ponderar o recurso a redes privadas para sistemas de proteção à distância, a fim de garantir o nível de qualidade de serviço requerido pelas restrições em tempo real. Ao utilizarem redes de comunicações públicas, os operadores devem ponderar a possibilidade de garantir a atribuição de largura de banda específica, requisitos de tempo de latência e medidas de segurança da comunicação;

   e) Dividir o sistema global em zonas lógicas e, dentro de cada zona, definir as condicionantes de tempo e dos processos, a fim de permitir a aplicação de medidas adequadas de cibersegurança, ou ponderar métodos de proteção alternativos.

5. Sempre que possível, os operadores de redes de energia devem também:

   a) Escolher um protocolo de comunicação seguro — tendo em conta os requisitos em tempo real —, por exemplo entre uma instalação e os seus sistemas de gestão (da energia/da distribuição);

   b) Adotar um mecanismo de autenticação adequado para a comunicação máquina-máquina, que satisfaça os requisitos em tempo real.

EFEITOS EM CASCATA

6. Os Estados-Membros devem assegurar que as partes interessadas, nomeadamente os operadores de redes de energia, os fornecedores de tecnologias e, em especial, os operadores de serviços essenciais identificados na Diretiva SRI, aplicam as medidas de preparação que se impõem em matéria de cibersegurança, relacionadas com os efeitos em cascata no setor da energia. As redes de eletricidade e os gasodutos estão fortemente interligados em toda a Europa, pelo que um ciberataque que crie uma falha ou perturbação numa componente do sistema energético pode desencadear efeitos em cascata de grande alcance noutras componentes desse sistema.

7. Ao aplicarem a presente recomendação, os Estados-Membros devem avaliar as interdependências e a criticidade dos sistemas de produção de energia e de procura flexível, das subestações e das linhas de transporte e distribuição, bem como das componentes conexas — inclusive transfronteiras — passíveis ser afetadas em caso de ciberataques ou ciberincidentes que tenham êxito. Os Estados-Membros devem também assegurar que os operadores das redes de energia dispõem de um quadro de comunicação com todas as principais partes interessadas, para partilhar os sinais de alerta precoce e cooperar em matéria de gestão de crises. Devem existir canais de comunicação estruturados e formatos normalizados para a partilha de informações sensíveis com todas as partes interessadas, as equipas de intervenção em caso de incidentes de segurança informática e as autoridades responsáveis.

8. Em especial, os operadores de redes de energia devem:

   a) Garantir que os novos dispositivos (nomeadamente no âmbito da «Internet das coisas») têm e mantêm um nível de cibersegurança adequado à importância crítica do local;

   b) Ponderar devidamente os efeitos ciberfísicos ao estabelecerem e reverem periodicamente os planos de continuidade das atividades;

c) Estabelecer critérios de conceção e uma arquitetura para uma rede resiliente, que possa ser alcançada através do seguinte:

— adoção de medidas de defesa aprofundadas por local, adaptadas à importância crítica deste;

— identificação de nós críticos, tanto em termos de capacidade de produção de energia como de impacto nos clientes. As funções críticas de uma rede devem ser concebidas para atenuar riscos que possam ter efeitos em cascata, providenciando redundâncias, resiliência a oscilações de fase e proteções contra cortes em carga em cascata.

— colaboração com outros operadores e fornecedores de tecnologias para evitar os efeitos em cascata, mediante a provisão de medidas e serviços adequados;

— conceção e construção de redes de comunicação e de controlo com vista a restringir os efeitos de eventuais falhas físicas e lógicas a certas áreas delimitadas das redes e a assegurar que sejam prontamente aplicadas medidas de atenuação adequadas.

TECNOLOGIAS ANTIGAS E DE PONTA

9. Os Estados-Membros devem assegurar que as partes interessadas, nomeadamente os operadores de redes de energia, os fornecedores de tecnologias e, em especial, os operadores de serviços essenciais identificados na Diretiva SRI, aplicam as medidas de preparação que se impõem em matéria de cibersegurança, relacionadas com a combinação de tecnologias clássicas e de ponta no setor da energia. Coexistem no sistema energético de hoje dois tipos diferentes de tecnologias: uma tecnologia mais antiga, com um tempo de vida de 30 a 60 anos – concebida antes de se aplicarem considerandos de cibersegurança – e equipamentos modernos, que refletem a tecnologia digital e os dispositivos inteligentes de ponta.

10. Ao aplicarem a presente recomendação, os Estados-Membros devem incentivar os operadores de redes de energia e os fornecedores de tecnologia a adotarem, sempre que possível, as normas internacionalmente aceites em matéria de cibersegurança. Por seu turno, as partes interessadas e os clientes devem adotar uma abordagem de cibersegurança na ligação de dispositivos à rede.

11. Em particular, os fornecedores de tecnologias devem fornecer gratuitamente soluções testadas para as questões de segurança nas tecnologias clássicas ou novas, logo que surja uma questão de segurança relevante.

12. Em especial, os operadores de redes de energia devem:

a) Analisar os riscos inerentes à ligação de dispositivos clássicos e do domínio da «Internet das coisas» e ter conhecimento das interfaces internas e externas e das suas vulnerabilidades;

b) Tomar medidas adequadas contra ataques malévolos provenientes de um grande número de aplicações ou dispositivos de consumo que possam ser controlados por entidades mal-intencionadas;

c) Estabelecer uma capacidade de monitorização e análise automatizada dos eventos relacionados com a segurança, em contextos clássicos e do domínio da «Internet das coisas», nomeadamente tentativas falhadas de iniciar sessões, alarmes de portas de abertura de cabinas ou outros eventos;

d) Realizar regularmente análises de riscos específicos de cibersegurança em todas as instalações antigas, especialmente ao ligar tecnologias clássicas e novas. Dado que as instalações antigas representam frequentemente uma grande parte dos ativos, a análise de riscos pode ser feita por classes destes;

e) Atualizar, sempre que possível, o *software* e o *hardware* dos sistemas clássicos e dos sistemas do domínio da «Internet das coisas», adotando a versão mais recente; ao fazê-lo, os operadores de redes de energia devem ponderar a adoção de medidas complementares, como a segregação dos sistemas ou a adição de barreiras de segurança externa, se a reparação e a atualização forem recomendáveis mas não forem possíveis (caso, por exemplo, de produtos incompatíveis entre si);

f) Formular os cadernos de encargos tendo em conta a cibersegurança, ou seja, exigindo informações sobre os elementos de segurança, a conformidade com as normas de cibersegurança vigentes, a garantia de um alerta contínuo, de reparação e de atenuação caso sejam detetadas vulnerabilidades, bem como a clarificação da responsabilidade dos vendedores em caso de ciberataques ou de incidentes;

g) Colaborar com os fornecedores de tecnologias para substituir os sistemas clássicos sempre que isso se justifique por razões de segurança, tendo em conta as funcionalidades críticas dos sistemas.

MONITORIZAÇÃO

13. Os Estados-Membros devem transmitir à Comissão, 12 meses após a adoção da presente recomendação e, posteriormente, de dois em dois anos, informações pormenorizadas sobre o estado de execução da presente recomendação, através do grupo de cooperação SRI.

REEXAME

14. Com base nas informações apresentadas pelos Estados-Membros, a Comissão analisará a aplicação da presente recomendação e avaliará a eventual necessidade de adotar novas medidas, após consulta dos Estados-Membros e das partes interessadas pertinentes.

DESTINATÁRIOS

15. Os destinatários da presente recomendação são os Estados-Membros.

Feito em Bruxelas, em 3 de abril de 2019.

Pela Comissão
Miguel ARIAS CAÑETE
Membro da Comissão