2017

XIV Forte de Copacabana Conference
International Security

4/6

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

Hagen Colberg

As Capacidades Europeias contra Ameaças Cibernéticas: Fortalecendo a Segurança de TI na Alemanha

The European Capabilities against Cyber Threats: Strengthening IT Security in Germany

Organisers

Konrad Adenauer Stiftung

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

Supported by

União Europeia

XIV Forte de Copacabana Conference
International Security

A Conferência de Segurança Internacional do Forte de Copacabana é um projeto euro-brasileiro organizado em conjunto pela Fundação Konrad Adenauer (KAS) e pelo Centro Brasileiro de Relações Internacionais (CEBRI), com apoio da Delegação da União Europeia no Brasil. A conferência é concebida como um fórum de diálogo entre a América do Sul e a Europa. Seu objetivo é reunir especialistas do setor governamental, acadêmico e privado para discutir assuntos atuais no âmbito de segurança que sejam de interesse comum aos parceiros dos dois lados do Atlântico. Desde seu início em 2003, a conferência se transformou, de uma reunião relativamente pequena, no maior fórum de segurança da América Latina. Na sua 14ª edição, a conferência de 2017 tem como tema 'Arquitetura de Segurança: um intercâmbio entre América do Sul e Europa'. A conferência é aberta ao público e os participantes são incentivados a participar ativamente das discussões. Como novidade para este ano, esta coleção de Policy Papers reflete os temas centrais do evento e pretende identificar desafios, bem como fazer recomendações políticas para o futuro. As edições anteriores da publicação sobre Segurança Internacional da Conferência do Forte de Copacabana podem ser acessadas na página oficial da KAS Brasil (www.kas.de/brazil).

The Forte de Copacabana International Security Conference is a joint Euro-Brazilian project organised by the Konrad Adenauer Foundation (KAS) in partnership with the Brazilian Center for International Relations (CEBRI) and supported by the Delegation of the European Union to Brazil. The conference is conceived as a forum for dialogue between South America and Europe. It aims to bring together experts from a wide range of government, academic and private-sector backgrounds to discuss current security-related issues which are of interest to the partners on both sides of the Atlantic. Since its inception in 2003, the conference has emerged from a relatively small gathering to Latin America's largest security forum to date. The topic of the 14th edition of the conference is 'Security Architecture: An Exchange between South America and Europe'. The conference is open to the public and the audience is encouraged to actively engage in discussions. As an innovation in 2017, this collection of Policy Papers reflects the major themes of the event and intend to identify challenges as well as make policy recommendations for the future. Previous volumes of the Forte de Copacabana International Security Conference publication can be accessed on the KAS-Brazil Office website (www.kas.de/brazil).

www.kas.de/brasil

Editor Editor
Dr. Jan Woischnik

Coordenação editorial Project Coordination
Diogo Winnikes
Reinaldo Themoteo

Colaboração Editorial Support
Diego Andrade de Freitas
Sebastian Breuer

Projeto Gráfico Design
Charles Steiman

Impressão Print
J. Sholna

Fundação Konrad Adenauer
Rua Guilhermina Guinle, 163
Botafogo CEP: 22270-060
Rio de Janeiro, RJ – Brasil
Tel: (+55/21) 2220-5441
Fax: (+55/21) 2220-5448

www.kas.de/brasil
kas.brasil
kasbrasil

ISSN 2176-297X

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

1/6
Perspectivas Sul-Americanas para uma Futura Cooperação em Arquitetura de Segurança: Arranjos, Processos e Desafios

South American Perspectives for Future Cooperation on Security Architecture: Arrangements, Processes and Challenges

Antonio Jorge Ramalho
Tradução e revisão Translation and Revision: Leslie Sasson Cohen

2/6
A Ordem de Segurança Global e Europeia na Crise: Poder, Instituições, Princípios

The Global and European Security Order during the Crisis: Power, Institutions, Principles

Markus Kaim
Tradução Translation: Tito Lívio Cruz Romão I Revisão Revision: Leslie Sasson Cohen

3/6
As Capacidades Sul-Americanas contra Ameaças Cibernéticas: Das Fragilidades Atuais a uma Resposta Comum

The South American Capabilities against Cyber Threats: From the Current Weaknesses towards a Common Response

María Lourdes Puente Olivera

Susana García
Tradução e revisão Translation and Revision: Leslie Sasson Cohen

4/6
As Capacidades Europeias contra Ameaças Cibernéticas: Fortalecendo a Segurança de TI na Alemanha

The European Capabilities against Cyber Threats: Strengthening IT Security in Germany

Hagen Colberg
Tradução Translation: Tito Lívio Cruz Romão I Revisão Revision: Leslie Sasson Cohen

5/6
O Nexo Transatlântico do Narcotráfico: a Visão Sul-Americana para uma melhor Colaboração entre a América do Sul e a Europa contra o Tráfico de Drogas

The Transatlantic Narco-Nexus: The South American View for better Collaboration between South America and Europe against Drug Trafficking

Thiago Rodrigues

Carol Viviana Porto
Tradução e revisão Translation and Revision: Leslie Sasson Cohen

6/6
A Perspectiva Europeia para uma melhor Colaboração entre a América Latina e a Europa no Combate ao Narcotráfico

The European View for better Collaboration between Latin America and Europe against Drug Trafficking

Mikael Wigell

Joren Selleslaghs
Tradução e revisão Translation and Revision: Leslie Sasson Cohen

A Fundação Konrad Adenauer (KAS) é uma fundação política alemã. Através do nosso escritório central na Alemanha e dos mais de 90 escritórios espalhados pelo mundo, gerenciamos mais de 200 projetos abrangendo mais de 120 países. Tanto na Alemanha quanto no exterior, nossos programas de educação cívica têm como objetivo promover os valores de liberdade, paz e justiça, bem como diálogo e cooperação. Como think tank e agência de consultoria, nós focamos na consolidação da democracia, na unificação da Europa, no fortalecimento das relações transatlânticas, assim como na cooperação internacional e no diálogo. Os nossos projetos, debates e análises visam o desenvolvimento de uma forte base democrática para ação política e cooperação.
No Brasil, nossas atividades concentram-se no diálogo de segurança internacional, educação política, estado de direito, funcionamento de instituições públicas e seus agentes, economia social de mercado, política ambiental e energética assim como as relações entre o Brasil, a União Europeia e a Alemanha.

The Konrad Adenauer Stiftung (KAS) is a German political foundation. From our headquarters in Germany and 90 field offices around the globe, we manage over 200 projects covering over 120 countries. At home as well as abroad, our civic education programmes aim at promoting the values of freedom and liberty, peace and justice, as well as dialogue and cooperation. As a think tank and consulting agency we focus on the consolidation of democracy, the unification of Europe, the strengthening of transatlantic relations, as well as on international cooperation and dialogue. Our projects, debates and analyses aim to develop a strong democratic base for political action and cooperation.
In Brazil our activities concentrate on international security dialogue, political education, the rule of law, the workings of public institutions and their agents, social market economy, environmental and energy policy, as well as the relations between Brazil, the European Union and Germany.

União Europeia

A Delegação da União Europeia (UE) no Brasil é uma das mais de 130 Delegações da UE no mundo. A Delegação da UE no Brasil está focada na promoção das relações políticas e econômicas entre a UE e o Brasil, de acordo com a parceria estratégica EU–Brasil estabelecida em 2007. A UE e o Brasil estabeleceram relações diplomáticas em 1960, criando estreitos laços históricos, culturais, econômicos e políticos. Dentre os tópicos centrais da parceria estratégica entre a UE e o Brasil estão questões econômicas, a cooperação em questões-chaves de política externa e o enfrentamento conjunto de desafios globais em áreas como direitos humanos, mudanças climáticas e a luta contra a pobreza. Mais de 30 diálogos formais no setor político foram iniciados entre a União Europeia e autoridades brasileiras para enfrentar esses desafios. Além disso, a União Europeia e o Brasil são parceiros comerciais importantes e os países da União Europeia recebem mais de 20% da exportação brasileira. A União Europeia também é o maior investidor estrangeiro no Brasil com cerca de 60% do investimento estrangeiro.

The European Union (EU) Delegation to Brazil is one of over 130 EU Delegations around the world. The EU Delegation to Brazil is focused on promoting political and economic relations between the EU and Brazil, in line with the EU–Brazil Strategic Partnership established in 2007. The EU and Brazil established diplomatic relations already in 1960 building on close historical, cultural, economic and political ties. Central topics of the EU–Brazil Strategic Partnership include economic issues, cooperation on key foreign policy issues, and jointly addressing global challenges in areas such as human rights, climate change as well as the fight against poverty. Over 30 formal sector-policy dialogues between the European Union and Brazilian authorities have been initiated to address these challenges. The European Union and Brazil are also important trading partners and the countries of the European Union account for over 20% of Brazil's exports. The European Union is also the largest foreign investor in Brazil with around 60% of the foreign investment originating from the European Union.

CEBRI
BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

Independente, apartidário e multidisciplinar, o Centro Brasileiro de Relações Internacionais (CEBRI) é uma instituição sem fins lucrativos, que atua para influenciar positivamente a construção da agenda internacional do país. Fundado há quase 20 anos por um grupo de empresários, diplomatas e acadêmicos, o CEBRI tem ampla capacidade de articulação, engajando os setores público e privado, a academia e a sociedade civil. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes, e com uma rede de mantenedores constituída por instituições, empresas e indivíduos de múltiplos segmentos.

O CEBRI promove a expansão e aprofundamento do debate sobre a política externa brasileira e a inserção do Brasil no mundo, pautado na formulação de políticas públicas e no fomento de diálogo entre os mais relevantes atores brasileiros e globais. O reconhecimento de sua importância internacional é atestado pelo ranking do Programa de Think Tanks e Sociedade Civil da Universidade da Pensilvânia, que destacou o CEBRI como o segundo melhor think tank do Brasil e o quarto melhor da América Latina.

Independent, nonpartisan and multidisciplinary, the Brazilian Center for International Relations (CEBRI) is a non-profit institution that acts to have a positive influence on the construction of the country's international agenda. Founded nearly 20 years ago by a group of business leaders, diplomats and academics, CEBRI has the ability to engage the public and private sectors, academia and civil society. In addition, it counts on an engaged Board of Trustees formed by prominent figures and on a diverse network of sponsors made up of institutions, companies and individuals from multiple sectors.

CEBRI promotes the expansion and deepening of debates on Brazilian foreign policy and Brazil's international insertion, marked by the formulation of public policies and the promotion of dialogue amongst the most relevant Brazilian and global stakeholders. The recognition of its international importance is evidenced by the University of Pennsylvania's Think Tanks and Civil Societies Program, which ranked CEBRI as Brazil's second best think tank and the fourth best in Latin America.

Hagen Colberg é conselheiro legislativo de Thomas Jazombek, Membro do Parlamento Federal Alemão (Bundestag) desde 2009 e porta-voz da Bancada Parlamentar CDU/CSU para a agenda digital. Ele começou a trabalhar no Parlamento Federal Alemão em janeiro 2011, após estudar na Universidade Martin Luther de Halle-Wittenberg e formar-se em Ciência Política na Universidade de Potsdam.

Hagen Colberg is a legislative adviser to Thomas Jarzombek, a Member of the German Federal Parliament (Bundestag) since 2009 and spokesman of the CDU/CSU parliamentary group on the digital agenda. He began working at the Bundestag in January 2011 after studying at the Martin Luther University in Halle (Saale) and graduating from Potsdam University with a diploma in Political Science.

As Capacidades Europeias contra Ameaças Cibernéticas: Fortalecendo a Segurança de TI na Alemanha

Hagen Colberg

The European Capabilities against Cyber Threats: Strengthening IT Security in Germany

In November 2016, there was the numerically largest attack ever against the internet infra structure in Germany. In the midst of the disaster, fortunately more than one million Deutsche Telekom routers were not part of a global botnet, which still resulted in damages which were estimated at several millions euros. The hacker, a 29-year-old British man, said in the investigation that he had acted on behalf of a Liberian businessman with the aim of adding the routers to an international botnet. At the end of July 2017, he was handed a suspended jail sentence of one year and eight months, and Great Britain requested his extradition on the basis of other crimes, which the young man had committed before[1]. In 2017, the ransomwares WannaCrypt (May 2017) and (Not) Petya (June / July 2017) shook the world. Even critical infrastructures were hit by the ransomware attack. In some companies in Germany the production or other critical corporate processes stopped partially for more than a week, causing millionaire losses, although the country had been relatively weakly affected[2]. In addition, news and reports are constantly circulating about the loss of user data on large Internet platforms; criminals paralyze websites of service providers, news agencies or other organizations, and even governments. Botnets are often used for such DDoS attacks. Threats are everywhere. But not everything is a hacking attack, there is not always a foreign cyber army behind the problem. However, changes that provide more security on the internet are yet to come. Last year, the preferred password for users around the world was "123456".

Digital Agenda and the IT Security Law

The IT Security Law was very important as a way to sensitize providers and users about the threats that successful attacks pose to critical IT systems infrastructures; this law was equally important to improve the defense capabilities, as critical infrastructures require well-functioning IT services, and also because we cannot exclude the possibility that they collapse. With the Digital Agenda, in 2014 the German Federal Government proposed, within the framework of an IT Security Law, to strengthen IT security by expanding partnerships with critical infrastructure providers and by creating legal requirements, in addition to introducing an obligation to report significant incidents in the IT area. Germany was a pioneer with the IT Security Law in 2015.[3] Through this law, critical infrastructure providers are required to ensure the security of their IT infrastructures according to the latest technology. The sectors concerned (information technology and telecommunications, energy management, food industry, water management, finance, transport and transit, as well as the health sector) have been defined in two regulations of the German Ministry of Interior, considering the quality and the amount of penetration rate achieved by systems, equipment or parts of critical infrastructures. The last regulation came into force at the end of June 2017. These IT Security Law regulations have been designed through dialogue with the areas involved, with a view to increasing the effectiveness of the measures. Non-registered systems will also always be able to join the cyber-security alliance, even if they are not critical infrastructures. Critical infrastructure providers situated below the limit values set out in the Regulation can join UP KRITIS, a public-private partnership of Critical Infrastructure Providers (KRITIS), its associations and state institutions.[4] These important factors must be emphasized: security measures also need to be realistic, and the conflict between user comfort and security must always be rebalanced. It makes no sense to maximize measures if users of IT infrastructures are virtually forced to seek out solutions through unsafe methods.

The European Union NIS Directive

Critical infrastructures cover power stations and hydroelectric power plants, airports, hospitals, banks and insurance companies. A collapse in these sectors can have very serious consequences for the day-to-day functioning and for the public safety as well – regardless of national laws. In February 2013, a draft directive on cybersecurity information was presented by the EU Commission and approved in 2016 (Directive EU

1 See the newspaper "Der Tagesspiegel": Bewährungsstrafe für Briten nach Hackerangriff, 28. Juli 2017, available at: http://www.tagesspiegel.de/wirtschaft/telekom-router-attackiert-bewaehrungsstrafe-fuer-briten-nach-hackerangriff/20120204.html

2 See the BSI's opinion on the Petya incident at https://www.bsi.bund.de/EN/Presse/Press Releases / Presse2017 / Update_Cyber_Angriffswelle_Petya_07072017.html

3 Documentation of the legislative procedure at http://dipbt.bundestag.de/extrakt/ba/WP18/643/64396.html

4 More about UP KRITIS at: http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html

Em novembro de 2016, ocorreu na Alemanha o maior ataque, em números, já realizado contra a estrutura da internet até hoje. Em meio ao desastre, felizmente mais de um milhão de roteadores da *Deutsche Telekom* não se tornou parte de uma botnet global, embora o prejuízo tenha sido milionário. O autor do ataque, um jovem britânico de 29 anos, declarou no inquérito ter agido em nome de um empresário liberiano com o objetivo de adicionar os roteadores a uma *botnet* internacional. No final de julho de 2017 ele foi condenado a um ano e oito meses de prisão em regime de liberdade condicional, e a Grã-Bretanha solicitou a sua extradição com base em outros delitos que o rapaz cometeu[1]. Em 2017, os *ransomwares WannaCrypt* (maio de 2017) e *(Not)Petya* (junho/julho de 2017) sacudiram o mundo. Até mesmo infraestruturas críticas foram atingidas pelo ransomware. Em algumas empresas na Alemanha a produção ou outros processos corporativos críticos pararam parcialmente durante mais de uma semana, provocando prejuízos milionários, embora o país tenha sido afetado de forma relativamente branda.[2] Além disso, sempre voltam a circular notícias sobre a perda de dados de usuários em grandes plataformas da internet; os criminosos paralisam os *websites* de prestadores de serviços, de agências de notícias ou de outras organizações e até de governos. No caso desses ataques DDoS, lançam mão de *botnets.* As ameaças estão por todos os lados. Mas nem tudo é um ataque de *hackers*, nem sempre há um exército cibernético estrangeiro por trás do problema. No entanto, ainda estão por vir mudanças que proporcionem mais segurança na internet. No ano passado, a senha preferida dos usuários em todo o mundo foi "123456".

Agenda Digital e a Lei de Segurança de TI

A Lei de Segurança de TI foi importante para sensibilizar operadores e usuários sobre os perigos de ataques bem-sucedidos contra os sistemas de TI de infraestruturas críticas e também para melhorar as capacidades de defesa, uma vez que as infraestruturas críticas sempre requerem serviços de TI operantes, já que nunca se pode excluir a possibilidades de falhas. Com a Agenda Digital, em 2014 o Governo Federal alemão se propôs, no âmbito de uma Lei de Segurança de TI, a fortalecer a segurança de TI expandindo parcerias com provedores de infraestruturas críticas e criando dispositivos legais, além de introduzir uma obrigatoriedade de notificação de incidentes significativos na área de TI. Em 2015, a Alemanha mostrou-se pioneira ao apresentar sua Lei de Segurança de TI.3 Através dessa lei, provedores de infraestruturas críticas são obrigados a garantir a segurança de suas infraestruturas de TI conforme a tecnologia mais recente. As áreas afetadas (tecnologia da informação e de telecomunicações, gestão energética, indústria alimentícia, gestão hídrica, finanças, transportes e trânsito, além do setor de saúde) foram definidas em duas regulamentações do Ministério do Interior alemão, considerando-se a qualidade e a quantidade da taxa de penetração alcançada pelos sistemas, equipamentos ou partes de infraestruturas críticas. A última regulamentação entrou em vigor no final de junho de 2017. Essas regulamentações da Lei de Segurança de TI foram concebidas através do diálogo com as áreas envolvidas visando a aumentar a eficácia das medidas. Equipamentos não registrados também poderão aderir à aliança de segurança cibernética a qualquer momento, mesmo quando não se tratar de infraestruturas críticas. Provedores de infraestruturas críticas situados abaixo dos valores-limite estabelecidos na regulamentação podem filiar-se à UP KRITIS, uma parceria público-privada de Provedores de Infraestruturas Críticas (KRITIS), às suas associações e às instituições estatais.4 Destaquem-se estes importantes fatores: as medidas de segurança também precisam ser sempre realistas, e o conflito entre conforto do usuário e segurança precisa sempre ser reequilibrado. Não faz nenhum sentido maximizar as medidas se os usuários de infraestruturas de TI praticamente se veem obrigados a buscar saídas através de soluções inseguras.

1 Cf. Jornal "Der Tagesspiegel" Bewährungsstrafe für Briten nach Hackerangriff [Prisão em regime de liberdade condicional para britânico após o ataque à rede de computadores, 28 de julho de 2017], acesso pelo link: http://www.tagesspiegel.de/wirtschaft/telekom-router-attackiert-bewaehrungsstrafe-fuer-briten-nach-hackerangriff/20120204.html

2 Cf. Declaração da BSI sobre o incidente do Petya pelo link: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Update_Cyber_Angriffswelle_Petya_07072017.html

3 Informações sobre os procedimentos legislativos através do link: http://dipbt.bundestag.de/extrakt/ba/WP18/643/64396.html

4 Maiores informações sobre a UP KRITIS pelo link: http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationaes/UPK/upk_node.html

2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union[5]). As the German IT Security Law served as a model for the NIS Directive negotiations at the European level, in Germany there was little demand when it was implemented. The involved providers commit themselves to evaluate their IT systems for possible vulnerabilities and, if necessary, to take additional protection measures. In addition, the reporting obligation extends to security events with considerable effects, including the possibility of anonymous notifications, provided there are no threats of a system crash. Here one can see clear parallels between the NIS Directive and the German IT Security Law. Just before the end of the legislative period, Germany had already transposed the NIS Directive of the European Union into German law. As a result, Germany was the first Member State to fulfill the requirements which will apply throughout the EU from May 2018 onwards.

The transposition law of the NIS Directive also allows the provision of protection services by the Federal Information Security Agency (BSI), aiming at recovering the security or functionality of IT systems at relevant events through the so-called Mobile Incident Response Teams (MIRT). In the past, some IT incidents have clearly shown that affected companies generally can only resort to insufficient protection. Operational experts who can be recruited for such cases are rare. The German Federal Ministry of the Interior and the BSI have therefore worked on a concept for the expansion of Mobile Incident Response Teams (MIRT) at BSI. With regard to this project, the German Parliament has already approved the necessary financial resources for the current year, we are now working on the legal requirements for implementation. Experts from the business world can thus be available with their know-how and additional staff and support the response teams of the BSI. Occasionally, these teams are referred to as cyber defense. The purpose of this cyber defense is to consist of voluntary and free-of-charge specialists from companies who are available to quickly remove the technical consequences of a successful IT attack. For this purpose, the BSI will enter into cooperative agreements with potential companies. In view of the high competition on the market of IT specialists, this is a comprehensible step.

The massive attack on Deutsche Telekom's Internet routers at the end of November 2016 has highlighted the significance that IT security measures have for a broad public. Unfortunately, botnet attacks are nothing new, but they are a source of great concern. Not only the infected laptop or PC can be the starting point of such attacks, but also IP cameras, printers with internet connection, routers or other more or less smart devices that are connected to the Internet. At the same time, it is predicted that the number of users without technical experience who use the devices in the standard configuration will increase. The dangers arising from such botnets are manifold. Currently, DDoS attacks on payment systems, web-shops, or other platforms are already a frequent problem. So it is right that we make a new regulation through a proposed amendment on how Internet service providers will be able to handle their networks in the future, so as to improve IT security starting with those who work on the network side. After all, not only should users be responsible for a secure network. In the future, network service providers, in order to inform users, should be able to redirect parts of the data transmission to and from a user where a malfunction has occurred (the so-called sink-holing). In this way, it will be possible to identify in your own network users with damaged systems and enabled to eliminate the malfunction. If a user does not disclose the existing problem, the network provider, provided that a malfunction is detected, shall be authorized to restrict, redirect or stop the transmission of data of the user in question or to filter the transmission of data to prevent threats caused by cyberattacks mainly to the provision of information and communication services.

In addition to the requirements contained in the NIS Directive, Germany has also intensified cooperation between the Federal Information Security Agency, which is responsible for protecting the Union's IT infrastructure, and the German federal states, in order to enable technical expertise to the states and thus be able to help them.

5 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016L1148

A Diretriz NIS da União Europeia

Infraestruturas críticas abrangem centrais elétricas e usinas hidrelétricas, aeroportos, hospitais, bancos e seguradoras. Um colapso nesses setores pode ter consequências muito graves para o funcionamento do nosso dia-a-dia e para a segurança pública – independentemente de leis nacionais. Em fevereiro de 2013, o anteprojeto de uma diretriz sobre segurança de informações cibernéticas foi apresentado pela Comissão Europeia e aprovada em 2016 (*Directive EU 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*[6*]). Como a Lei de Segurança de TI alemã serviu de modelo para as negociações da Diretriz NIS[7**] na esfera europeia, na Alemanha houve pouca demanda quando de sua implementação. Os provedores envolvidos se comprometem a avaliar seus sistemas de TI quanto a possíveis vulnerabilidades e, se necessário, adotar medidas de proteção adicionais. Além disso, a obrigatoriedade de notificação se estende a eventos de segurança com implicações significativas, admitindo-se a possibilidade de notificações anônimas, contanto que não haja ameaças de um colapso do sistema. Aqui se podem ver claros paralelos com a Lei de Segurança de TI alemã. Ainda antes do fim do período legislativo, a Alemanha transformou em lei alemã a Diretriz NIS da União Europeia. Com isso, a Alemanha foi o primeiro Estado-membro a cumprir os requisitos que passarão a ter validade em toda a UE a partir de maio de 2018.

A lei de implementação da Diretriz NIS possibilita também a prestação de serviços de proteção por parte da Agência Federal de Segurança em Tecnologia de Informação (BSI), visando à recuperação da segurança ou da operacionalidade de sistemas de TI em eventos relevantes por meio das chamadas equipes de atendimento móvel em caso de incidentes (*Mobile Incident Response Teams* ou simplesmente MIRT). No passado, alguns incidentes de TI mostraram claramente que as empresas afetadas em parte somente conseguem recorrer a um tipo de proteção insuficiente.

Raros são os peritos que podem ser recrutados para atuarem operacionalmente nesses casos. Por esse motivo, o Ministério do Interior alemão e a BSI elaboraram um projeto de expansão das MIRT junto à BSI. Com relação a esse projeto, o Parlamento Alemão já aprovou os recursos financeiros necessários para o ano em curso, agora estamos trabalhando nos requisitos legais para a implementação. Especialistas do setor empresarial também podem disponibilizar seu know-how e recursos humanos adicionais e assim apoiar as equipes de atendimento móvel da BSI. Essas equipes, que costumam ser chamadas de ciberdefesa, deverão ser compostas por especialistas de empresas que se colocam espontânea e graciosamente à disposição e que poderão atuar na rápida eliminação de implicações técnicas decorrentes de um ataque cibernético bem-sucedido. Para alcançar essa meta, a BSI firmará acordos de cooperação com empresas potenciais. Em virtude da grande competitividade na área de técnicos em TI, essa medida não encontra obstáculos.

O ataque em massa aos roteadores da *Deutsche Telekom* no final de novembro de 2016 também tornou evidente para um público mais amplo a importância que têm medidas visando à segurança de TI. Infelizmente, ataques de *botnets* não são nenhuma novidade, mas, muito mais, motivo para grandes preocupações. O ponto de partida desses ataques não precisa mais ser o laptop ou o PC infectado, mas também câmeras IP, impressoras conectadas à internet, roteadores ou outros aparelhos mais ou menos inteligentes com conexão à internet. Ao mesmo também há prognósticos de que aumentará o número de usuários sem experiência técnica que conectam os aparelhos na configuração-padrão à rede. Os perigos advindos dessas botnets são múltiplos. Atualmente, ataques DDoS a sistemas de pagamento, webshops ou outras plataformas já configuram um problema frequente. Por isso, é correto que façamos uma nova regulamentação através de uma proposta de emenda sobre a forma como os provedores de internet futuramente poderão lidar com suas redes, para assim, aprimorar a segurança de TI a partir de quem trabalha do lado da rede. Afinal de contas, não apenas os usuários devem ser responsáveis por uma rede segura. No futuro, prestadores de serviços de rede, com o intuito de informar os usuários, deverão ser capazes de redirecionar partes da transmissão de dados de e para um usuário

5 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016L1148

6 *N.T.: Diretriz UE 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, sobre medidas visando a um grau comum de segurança em sistemas cibernéticos e de informação em toda a União.

7 **N.T.: As letras NIS equivalem a: "network and information systems" (sistemas de redes e informação).

The Internet of (unsafe) Things?

The Internet of Things is the next generation of technology, and so new measures are needed to increase IT security. IT incidents that occurred up to now have caused several financial damages to varying degrees. In Germany, these losses amounted to EUR 55 billion over the last two years through corporate espionage, sabotage or data theft[6], although there has rarely been material damages or personal injuries. But the Internet of Things will connect devices that, if they happen to fail, can also have life-threatening consequences. If a self-driving car can be controlled by a third party[7] or a patient's insulin pump can be manipulated online[8], it will be necessary to have a debate about the redistribution of responsibilities between manufacturers and users. This is based on the assumption that the damages that could be caused to users or customers are only actually taken into account when they also mean any direct or indirect costs to the producer. In the United States, too, a draft was recently submitted to the Senate to improve security on the Internet of Things. In the case of purchases in the Internet of Things, the template presents new requirements to the suppliers, who in the future must meet minimum requirements for IT security; furthermore, the products are supposed to receive updates.[9]

Redistributing responsibility and creating transparency

For years it has been possible to observe a certain *laissez-faire* on the part of certain producers. The cyber security strategy of the Federal Government 2016 therefore provides guidelines for an appropriate distribution of responsibilities and security risks in the network. Already during the implementation of the NIS Directive in Germany there were proposals for further far-reaching regulations on the Internet of Things. Everything shall be interconnected, but what is interconnected will also be susceptible to attack. Therefore, there is a need for a proper distribution of responsibility between users and IT product manufacturers. This means product liability rules for IT security deficiencies and security precautions for hardware and software manufacturers on the Internet of Things. Some publications are talking about market failures, which would justify a European intervention.10 In this way, IT security will have to be integrated very early in the development of a product. Unfortunately, on the issue of IT accountability, no consensus was reached on the implementation of the NIS Guideline. In the view of parts of the government coalition, the European Union would be exclusively responsible for this. This is to be regretted, since national solutions can also become a European model. Here we can imagine claims for damages concerning the obligation to accept the return of products by the manufacturers, if during the normal period of use of a product it is no longer possible to make safety updates available, or if manufacturers do nothing against disclosed safety gaps. For this reason, binding criteria are required for networked IT products.

Quality seal for IT products

The proposed optional seal of approval is a further step towards improving IT security. Therefore, the German Federal Government's current cyber-security strategy correctly implies that the security of IT products and services needs to be presented more transparently to all citizens, as well as to small and medium-sized enterprises. For this purpose, quality seals and certifications for IT security should be developed. IT products must be evaluated in the interplay of software and hardware with their appropriate use or implementation. With the IT basic protection or the ISO 27001, basic criteria for IT security are already in practical use.

In the future, when deciding to purchase new IT products and making use of this kind of services, users will be able to quickly and easily determine which offer is securely designed and which thereby contributes to the protection of the data, on the basis of a uniform quality seal. To obtain the quality seal, the manufacturer of an IT product should make it clear that it works with security updates. In addition, the

6 Study of the IT association BITKOM from July 2017. More information at: https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html

7 See WIRED, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

8 See The Register, https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

9 See: Senate Cybersecurity Caucus, at: https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36

10 Paul-Jasper Dittrich: Die EU und die Sicherheit im Internet der Dinge [The EU and security on the Internet of things], available under: http://www.delorsinstitut.de/publikationen/alle-publikationen/die-eu-und-die-sicherheit-im-internet-der-dinge/

onde tenha sido originada uma avaria (o chamado *sinkholing*). Desse modo, será possível identificar em sua própria rede usuários com sistemas danificados e habilitados a eliminar a avaria. Caso um usuário não se manifeste, o provedor de rede, se for detectada uma avaria, deverá ser autorizado a restringir, redirecionar ou parar a transmissão de dados do usuário em questão ou ainda filtrar a transmissão de dados, para prevenir ameaças causadas por ataques cibernéticos sobretudo à disponibilização de serviços de informação e comunicação.

Além dos dispositivos contidos na Diretriz NIS, a Alemanha também intensificou a cooperação entre a Agência Federal de Segurança em Tecnologia da Informação, que é responsável pela proteção da infraestrutura de TI da União, e os estados federados, para possibilitar expertise técnica aos estados e assim poder ajudá-los.

A Internet das coisas (inseguras)?

A internet das coisas é a próxima geração da tecnologia, e por isso se fazem necessárias novas medidas que aumentem a segurança de TI. Incidentes de TI ocorridos até o presente momento provocaram prejuízos financeiros de diferentes dimensões. Na Alemanha, esses prejuízos chegaram, nos dois últimos anos, à casa dos 55 bilhões de euros através de espionagem empresarial, sabotagem ou roubo de dados[8], embora raramente tenha havido danos materiais ou contra pessoas. Porém, a internet das coisas conectará aparelhos que, se entrarem em colapso, também poderão representar ameaças à vida humana. Se o veículo autodirigido puder ser controlado por terceiros[9], ou se a bomba de insulina de um paciente puder ser manipulada *online*[10], será preciso fazer um debate sobre a divisão das responsabilidades entre fabricantes e usuários. Isso está em conformidade com a ideia de que prejuízos potenciais para usuários e/ou clientes somente são realmente levados em consideração quando associados a custos diretos ou indiretos para o produtor. Recentemente, nos Estados Unidos também foi apresentado ao Senado um anteprojeto visando a melhorar a segurança na internet das coisas. No caso de compras na área da internet das coisas, a proposta apresenta novas exigências aos fornecedores do serviço, que no futuro terão de satisfazer requisitos mínimos à segurança de TI, e os produtos poderão ser atualizados.[11]

Redistribuir as responsabilidades e gerar transparência

Há anos é possível observar uma certo laissez-faire por parte de determinados produtores. Por essa razão, a estratégia de segurança cibernética do Governo Federal alemão em 2016 conta com dispositivos para uma distribuição adequada das responsabilidades e das ameaças à segurança na rede. Já durante a implementação da Diretriz NIS na Alemanha surgiram propostas de regulamentações de maior alcance para a internet das coisas. Tudo será interconectado, mas o que estiver interconectado também será passível de ataques. Por conseguinte, faz-se necessário um debate sobre uma distribuição correta das competências entre usuários e fabricantes de produtos de TI. Isso significa regras de responsabilidade sobre produtos quanto a falhas de segurança de TI e também dispositivos de segurança para produtores de *hardwares* e *softwares* na internet das coisas. Algumas publicações falam de fracassos mercadológicos, que servem de base para uma interferência europeia12. Dessa maneira, a segurança de TI já terá de ser integrada bem cedo ao desenvolvimento de um produto. Infelizmente, no tocante ao tema da responsabilidade de TI, não se conseguiu um consenso na implementação da Diretriz NIS. Na opinião de partes da coalizão governamental, essa responsabilidade caberia apenas à União Europeia. Isso é lamentável, pois soluções nacionais também podem tornar-se um modelo europeu. Aqui podemos imaginar pedidos de indenização no âmbito da obrigatoriedade de aceitar a devolução de produtos por parte dos fabricantes, se durante o período normal de uso de um produto não for mais possível disponibilizar atualizações de segurança, ou se os fabricantes nada

8 Estudo da associação de TI BITKOM, julho de 2017. Maiores informações pelo link: https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html

9 Cf. WIRED, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

10 Cf. The Register, https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

11 Cf. Senate Cybersecurity Caucus, unter https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36

12 Paul-Jasper Dittrich: Die EU und die Sicherheit im Internet der Dinge [A UE e a segurança na internet das coisas], pelo link: http://www.delorsinstitut.de/publikationen/alle-publikationen/die-eu-und-die-sicherheit-im-internet-der-dinge/

seal should be tailored to the latest technology on the market in order to be able to provide relevant information that meet the consumers' purchasing decision and criteria, and which should also indicate an expiration or validity date when awarding the contract. Next year, BSI will conduct a first test with internet routers.[11]

Conclusion

It is necessary to make IT security more intelligible and easily achievable for anyone. Consequently, both enterprises and society at large would increase their confidence in digital safety. Attacks perpetrated against IT systems also ignore international borders; in addition to that, the existence of different laws and regulations with different degrees of severity give enough freedom for some perpetrators to escape criminal prosecution. That is why there is a need for European and international cooperation.

IT security is an ongoing task for the state and the economy. The solutions described above will not work in the long term if the users are not adequately provided with more awareness and information on IT security and if the various threats at all levels cannot be addressed.

11 Newspaper Wirtschaftswoche (25.08.2017) Neues Gütesiegel kommt 2018 [New seal of approval comes in 2018], at: http://www.wiwo.de/unternehmen/it/it-sicherheit-neues-guetesiegel-kommt-2018/20233314.html

empreenderem contra lacunas de segurança expostas. Consequentemente, são necessários critérios para produtos de TI conectados à rede.

Selo de qualidade para produtos de TI

O selo de qualidade opcional proposto é mais um passo rumo ao aprimoramento da segurança de TI. Por conseguinte, a atual estratégia de segurança cibernética do Governo Federal alemão entende corretamente que a segurança de produtos e serviços de TI precisa ser apresentada com maior transparência às cidadãs e aos cidadãos, bem como às pequenas e médias empresas. Nesse sentido, estima-se que serão desenvolvidos selos de qualidade e certificados referentes à segurança de TI. Desse modo, produtos de TI deverão ser avaliados em sua interação com softwares, hardwares e com sua adequada utilização e implementação. Através da proteção básica de TI e/ou com a ISO 27001, critérios fundamentais de segurança de TI já estão sendo aplicados na prática.

No futuro, os operadores, ao decidirem a compra de novos produtos de TI e ao fazerem uso de serviços prestados nessa área, poderão rápida e facilmente constatar, com base em um selo de qualidade unificado, qual oferta apresenta segurança e contribui para a proteção dos dados. Para a obtenção do selo de qualidade, o fabricante de um produto de TI deverá deixar claro que trabalha com atualizações de segurança. Além disso, o selo deverá ser adequado à tecnologia mais recente do mercado, para ser capaz de prestar informações relevantes que atendam às decisões de compras dos consumidores, e também deverá apresentar uma data de validade ou expiração no momento da concessão. No próximo ano, a BSI realizará um primeiro teste com roteadores de internet.[13]

Considerações finais

É necessário tornar a segurança de TI mais inteligível e facilmente realizável para qualquer pessoa. Isso aumenta a confiança na digitalização segura tanto para as empresas quanto para a sociedade em geral. Ataques de TI também ignoram as fronteiras, e a existência de diferentes leis e regulamentações com diferentes graus de rigor deixa margens para que os criminosos possam escapar à persecução penal. Por esse motivo, necessitamos de uma cooperação europeia e internacional.

Segurança de TI é uma tarefa permanente, tanto para o Estado quanto para as empresas. As soluções acima descritas não funcionarão em longo prazo se não for realizado de maneira adequada um trabalho de esclarecimento e conscientização dos usuários sobre segurança de TI, e se não forem enfrentadas as diferentes ameaças em todas as esferas.

13 Jornal “Wirtschaftswoche” (25.08.2017). Novo selo de qualidade chega em 2018. Acesso pelo link: http://www.wiwo.de/unternehmen/it/it-sicherheit-neues-guetesiegel-kommt-2018/20233314.html