d+i desenvolvendo ideias
LLORENTE & CUENCA

» Riscos cibernéticos e o novo paradigma da reputação

Madri » 05 » 2017

“A Espanha é o quinto país do mundo com o maior número de sistemas que controlam instalações e processos industriais conectados à internet, a maioria sem proteção”.[1] Esta é a opinião de Mercè Molist, uma jornalista especializada em ciberameaças. No ano passado, segundo dados fornecidos por ela, os ciberataques tiveram um aumento de 357 % na Espanha. Mesmo que esse número possa parecer exagerado, os números fornecidos pelo Instituto Nacional de Cibersegurança da Espanha (INCIBE) al de Ciberse mostram que, somente no ano passado, os ataques aumentaram de 50.000 para mais de 120.000. As empresas estão prontas para responder ao desafio de proteger sua reputação? Para algumas delas, a resposta será positiva; mas as mudanças regulatórias da Diretiva de segurança de redes e sistemas de informação e do novo Regulamento Europeu de Proteção de Dados Gerais (GDPR) poderá inibir outras empresas. Vamos tentar esclarecer tudo isso a seguir.

Não é novidade que as empresas enfrentam hoje um nível extremamente elevado de vulnerabilidade digital, basta mencionar três exemplos. O ataque mais recente foi há poucos dias, causado pelo worm WannaCry, que afetou mais de 150 países. O ataque de negação de serviço no ano passado atingiu os servidores da Dym nos Estados Unidos. Esse incidente sozinho afetou

um bilhão de usuários de empresas como Twitter, Amazon, Whatsapp e New York Times. É interessante lembrar também como os cibercriminosos atacaram caixas eletrônicos remotamente, forçando-os a “cuspir” dinheiro, em mais de uma dúzia de países da Europa. E isso foi apenas o começo.

Para tentar limitar os danos, promover uma cultura de gestão de riscos e garantir a notificação dos incidentes, foi adotada uma nova Diretiva de segurança das redes e sistemas de informação e um novo Regulamento Europeu para a Proteção de Dados que entrarão em vigor até 2018. Estes dois regulamentos estão sendo incorporados à legislação espanhola e representam uma mudança significativa nas culturas das empresas em termos de privacidade, direitos e obrigações na segurança do processamento digital de dados pessoais e prestação de serviços.

Esse regulamento estabelece que, até maio de 2018, a organização será obrigada a notificar, em menos de 72 horas, ao CERN (ou órgão designado) e às partes afetadas, qualquer tipo de falha na segurança resultante de ciberataques ou incidente interno. Se não souber quais dados pessoais do cliente estão comprometidos, a organização também deverá trazer essa situação para o conhecimento público.

> – Como assim? Se eu fizer isso, todo mundo vai saber que os dados dos meus clientes estão comprometidos e logo depois dezenas de jornalistas estarão lá fora pedindo uma explicação.

– É isso mesmo. Esta é a ideia.

Para esclarecer, vamos usar um exemplo: se um banco que tiver dados de clientes roubados não puder estabelecer quantos clientes foram afetados pelo ataque, então o banco deve informar todos eles.

Não importa se isso for feito publicamente ou não. A partir desse momento, as mídias sociais farão o resto. Poucos minutos depois, essa informação estará online e a mídia estará ciente disso. Sem dúvida alguma, a reputação e o valor das ações da sua empresa (se sua empresa operar na bolsa) serão afetados.

---

[1] *La ciberseguridad de la industria española es un sainete, y los ataques se están disparando* Mercè Molist 2017 http://www.elconfidencial.com/tecnologia/2017-03-20/ciberseguridad-industria-espanola-infraestructuras-criticas_1350398/

MULTAS

– Tem mais ainda?

– Com certeza. Um regulamento sem penalidades não pode ser chamado de regulamento. Segundo o novo Regulamento Europeu de Proteção de Dados, além de ser atacado por hackers, podem ser aplicadas multas de milhões de euros, ou 4 % do faturamento geral anual.

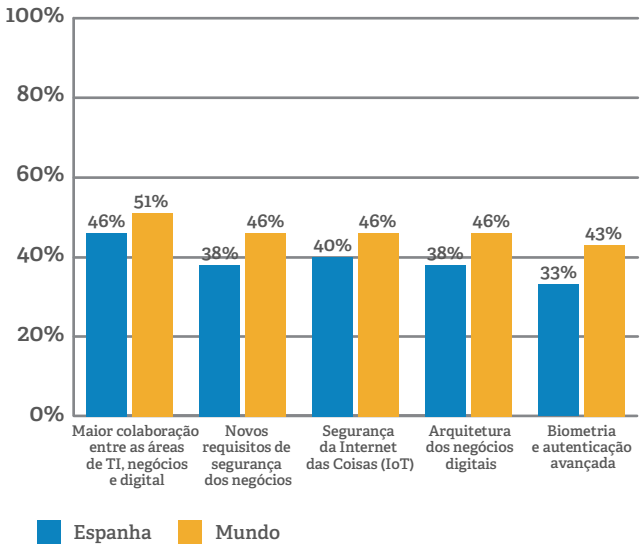
Alguns Diretores de Segurança da Informação (CISO) têm falado publicamente que esta lei é uma verdadeira chantagem, que pode tirar muitas empresas do mapa e beneficiar ainda mais a formação de oligopólios.

> “Segundo o novo Regulamento Europeu de Proteção de Dados, além de ser atacado por hackers, podem ser aplicadas multas de milhões de euros, ou 4 % do faturamento geral anual”

– Mas, espera, você ainda terá que pagar um pouco mais; você já ouviu falar sobre o Diretor de Proteção de Dados? Todas as empresas serão obrigadas a manter este cargo, dentro ou fora da organização. Esse profissional será o único porta-voz para todos estes assuntos e será encarregado de informar às organizações e autoridades competentes todos os ataques sofridos e qualquer divulgação de dados que possa ter ocorrido.

– IPs são considerados dados pessoais. Isto é, devem ser disponibilizados novos procedimentos específicos de prevenção, proteção de dados e gerenciamento de ciberataques. Isso envolverá sistemas específicos de documentação, notificação e comunicação. Algumas empresas de grande porte, que sofrem dezenas de ataques todos os dias, terão que criar unidades específicas cuja tarefa principal será relatar os ataques sofridos à autoridade competente e, ocasionalmente, aos clientes.

Figura 1. Onde as empresas investirão em termos de cibersegurança nos próximos doze meses?



Fonte: PwC, *The Global State of Information Security Survey 2017.*

UM NOVO PARADIGMA DE SEGURANÇA

Desta forma, é importante estar informado sobre o novo **paradigma de comunicação que estamos presenciando, que é caracterizado pela informação simultaneamente digital, online e líquida, inserida em uma estrutura hipertransparente.**

Hoje somos grandes meios de comunicação graças aos nossos dispositivos móveis, mas também nos tornamos, pela mesma razão, grandes riscos para cada organização da qual fazemos parte, as nossas e de outros. Somos um verdadeiro vetor de risco. E o nosso PC não é exatamente o ponto mais crítico. Provavelmente, ele está sob a forte vigilância da equipe de TI. Mas, e os nossos celulares ou tablets?

O paradigma de segurança não se adaptou à nova dinâmica: comportamento social digital, mobilidade, nuvem e informação (Big Data). Passamos os últimos anos discutindo processos de transformação digital em todas as organizações, mas esquecemos de cuidar dos riscos associados a estas mudanças. A alta complexidade dos quatro elementos mencionados acima irá alterar toda a abordagem de precaução, pois o escopo a ser protegido é agora mais amplo. Na verdade, é um perímetro global. As nossas conexões são globais, e assim como somos capazes de viralizar uma informação em tempo real; uma ameaça pode ser disseminada em todo o mundo em questão de segundos.

Portanto, é normal que, quando ocorre essa vulnerabilidade, os governos tomem medidas para proteger o sistema, as organizações e as empresas, para definir toda a rastreabilidade dos dados. Porém, a adoção de controles nessas circunstâncias colocará fortes limites aos direitos e liberdades. É só uma questão de tempo até começarmos a sofrer controles mais rígidos. Como vimos recentemente, após os ataques em Berlim, as autoridades alemãs estavam pedindo acesso aos dados do WhatsApp para combater os terroristas. Com os ciberataques não será diferente; ao contrário, será uma nova motivação. O que está em jogo é a segurança das infraestruturas essenciais, do sistema financeiro e, é claro, dos cidadãos.

Com isso, não vai demorar muito para vermos diferentes níveis de acesso aos dados, o que envolverá a definição de novas classes cibersociais. Diferentes perfis de acesso, serviços e taxas, dependendo da interação dos dados; o que acabará gerando castas sociais de acordo com o nosso nível de vulnerabilidade.

A NOVA LICENÇA SOCIAL NECESSÁRIA PARA OPERAR

A licença social para operar não estará mais condicionada à necessidade de proteger a nossa reputação. Como estão sempre sob a supervisão do órgão regulador, as empresas serão obrigadas a provar constantemente que protegem os dados dos clientes de forma eficiente, e que são capazes de manter seus sistemas em operação. Isso implica uma mudança de cultura da empresa, favorecendo uma responsabilidade proativa. A inspeção permanente do órgão regulador e a constante notificação aos clientes farão com que as empresas mudem seu DNA, tornando-as mais transparentes e colaborativas. Na verdade, apenas

as empresas que conseguirem se adaptar a este novo cenário poderão continuar operando no mercado. Tudo isso trará mudanças na forma como as coisas são ditas, dando origem à nova narrativa de sustentabilidade.

Infelizmente, nos últimos anos, temos visto como os gestores de algumas grandes empresas, tanto nacionais quanto internacionais, colocam o seu interesse pessoal acima do interesse dos acionistas e de outros grupos de interesse. Esses casos, quando a supervisão não cumpre com seus objetivos, podem causar resultados devastadores, como os casos infelizes de empresas que ruíram de forma dramática (Enron, Afinsa, Pescanova e Gowex, entre outros).

Para concluir, poderíamos dizer que, embora a essência da sustentabilidade compreensiva tenha sido sempre latente, agora está finalmente sendo revelada. Hoje enfrentamos novos desafios, novos públicos, novos conteúdos e um interesse crescente sem precedentes. Essencialmente, considerando este novo cenário de sustentabilidade, nada muda, mas nada permanece igual.

> "Segundo informações publicadas pela *PR Newswire*, em 2016, 90 % dos ciberataques foram causados por informações roubadas de funcionários, depois que seus sistemas foram invadidos"

O FUNCIONÁRIO, O ELEMENTO MAIS VULNERÁVEL

De acordo com dados coletados pela IBM em 2016, dois terços dos ataques às empresas foram realizados por agentes internos[2]. Segundo informações publicadas pela *PR Newswire*, em 2016, 90 % dos ciberataques foram causados por informações roubadas de funcionários, depois que seus sistemas foram invadidos. Portanto, não é surpresa alguma que, de acordo com o barômetro Allianz de Riscos para 2017[3], os danos à reputação foram a principal causa de perdas em 69 % das empresas que haviam sofrido ataques.

Portanto, em nossa opinião, o novo paradigma do risco à reputação leva ao fato de que os indivíduos com acesso aos dados da empresa podem reescrevê-los, o que, ao mesmo tempo, implica reescrever a reputação dessa empresa. Por isso, a proteção adequada dos dados da empresa será uma condição necessária para preservar a sua reputação.

Assim que estiverem cientes desses riscos, os CEOs e as empresas não terão outra escolha senão liderar a segurança digital; este será um aspecto transversal de toda a organização, pois não se trata de um assunto com o qual apenas o departamento de TI deve se preocupar-se, para atender aos requisitos de regulamentos e proteger a reputação. Na verdade, a confiabilidade corporativa dividirá as empresas em dois grupos: o grupo de empresas preparadas para enfrentar as ciberameaças e o grupo de empresas que não preparadas.

SINTOMAS DO CIBERESTRESSE REPUTACIONAL

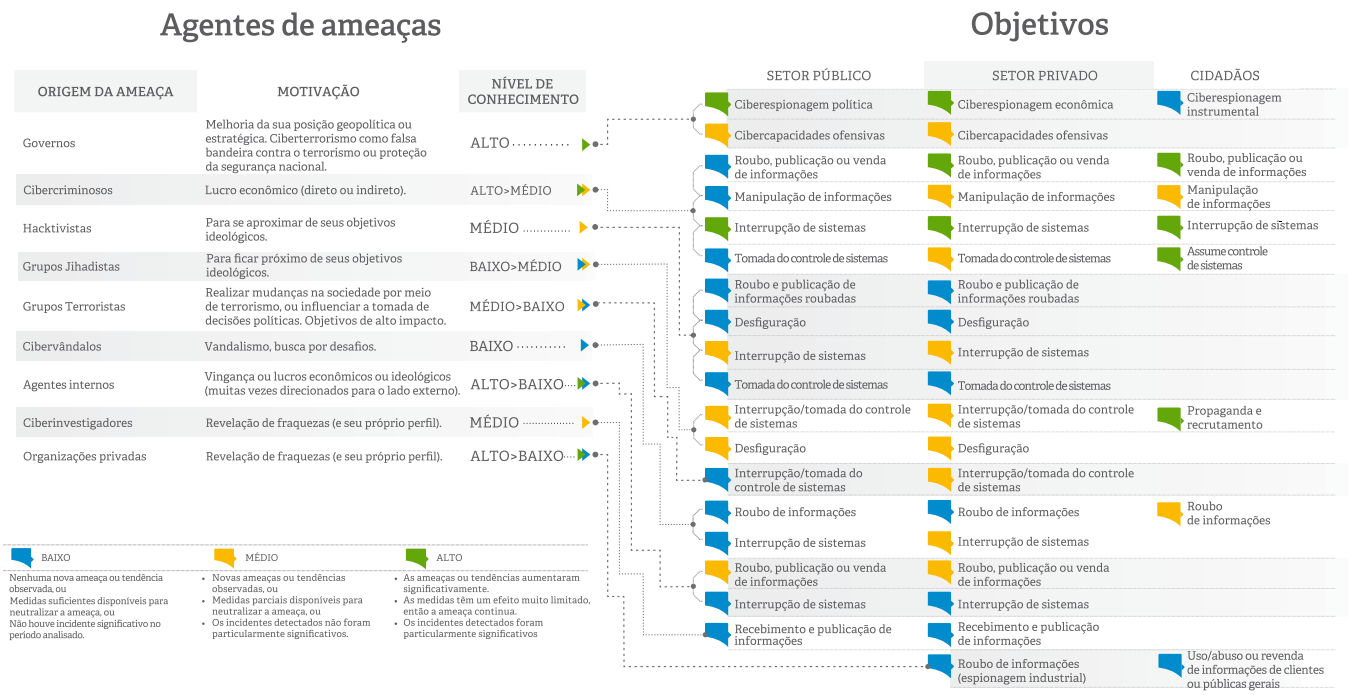
O novo paradigma de ciber-riscos criará um alto nível de estresse na organização, que será motivado por:

- Aumento da pressão de órgãos reguladores e adaptação técnica e organizacional a essas novas medidas legais.

[2] Segundo a IBM, os dados comprometidos por ciberataques aumentaram 566 % em 2016. Telam 2017 http://www.telam.com.ar/notas/201704/185558-ciberataques-seguridad-crecimiento-2016-informe-ibm-sector-financiero.html

[3] *Allianz Risk Barometer 2017*, Allianz 2017 http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2017/

Figura 2. Agentes de ameaças.



Fuente: CN-Cert, Centro criptológico nacional.

- Aumento do estresse no ambiente interno das empresas. A necessidade de proteger o usuário final e compreender que cada funcionário representa um risco em sua estação de trabalho e em seus dispositivos móveis.
- Maior pressão corporativa na gestão corporativa, devido à hipervulnerabilidade, em detrimento ao valor das organizações.
- Ausência de uma barreira de proteção sólida para a reputação, que garanta a identificação de riscos potenciais e procedimentos operacionais preventivos da administração para cada ciberameaça, do ponto de vista da gerência e da comunicação.

> "Além do desempenho financeiro adequado, os acionistas e os investidores exigem uma conduta cada vez mais responsável"

RISCOS À REPUTAÇÃO, NO NOVO PARADIGMA DE CIBER-RISCOS

Como resultado desse novo cenário, os riscos à reputação que tradicionalmente afetavam a empresa aumentarão a partir de agora, e terão duas direções:

- Comunicação e notificação permanentes das empresas, com relação a todos os ataques sofridos e as dificuldades que enfrentam para garantir a proteção dos dados; isso envolverá uma crescente falta de confiança decorrente da vulnerabilidade da empresa. Os usuários exigirão mais garantias de proteção de dados e recorrerão às grandes empresas que lhes ofereçam mais garantias.
- As empresas terão que desenvolver novos procedimentos de comunicação com seus clientes, utilizando todos os canais disponíveis para mantê-los informados em tempo real e com segurança e evitar que os meios de comunicação se concentrem em suas vulnerabilidades. Isso exigirá um reforço das equipes de comunicação e um fluxo contínuo de informações. Críticas online ocorrerão a qualquer momento e devem ser neutralizadas o mais rápido possível. A exposição pública está aumentando e, portanto, é necessário estar pronto a qualquer momento.

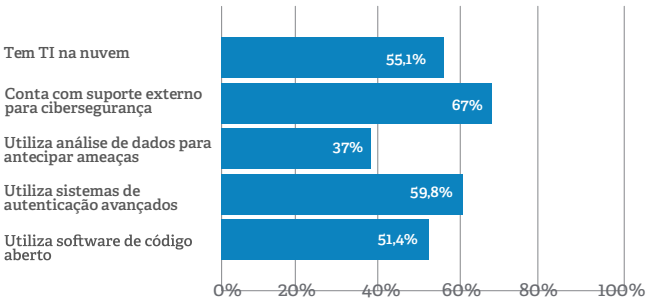
COMO ENCARAR ESTE NOVO CENÁRIO DE CIBER-RISCOS À REPUTAÇÃO?

Depois de analisar este novo cenário de riscos à reputação, que as empresas em breve terão que enfrentar, é óbvio que a única solução é realizar uma preparação multidisciplinar que possa reduzir os riscos. Com relação a isso, algumas medidas para tratar os temas analisados são as seguintes:

- **Proteção dos dados**: investir em especialistas de TI, aumentar os investimentos em tecnologias de proteção e, acima de tudo, melhorar a cultura de prevenção das empresas.
- **Proteção de evidências no caso de ataque**: com equipes multidisciplinares compostas por pessoas dos departamentos de TI, jurídico e financeiro; melhorando assim todos os processos de treinamentos internos para promover uma cultura de proteção com testes entre os funcionários. Para isso, será fundamental testar as ferramentas de proteção disponíveis, para posterior análise forense.
- **Big data e inteligência artificial:** aplicados na análise de grandes volumes de dados, implementando a melhor tecnologia disponível para elaborar relatórios sobre riscos e danos sofridos.
- **Pressão de órgãos reguladores:** ter especialistas em conformidade e proteção de dados. Será necessário melhorar as relações com os órgãos reguladores e de supervisão.
- **Estresse na organização:** foco na modificação dos processos internos de gestão a organização, envolver o departamento de Recursos Humanos, criar uma Comissão de Crises, cujos membros são treinados sobre as ciberameaças, melhorar o treinamento preventivo interno dos funcionários e estabelecer requisitos rigorosos.
- **Pressão corporativa:** aumentar todos os canais de informação que permitem neutralizar a percepção do risco de investimento, apresentar relatórios que comprovam como os dados, os testes e a reputação são protegidos.
- **Risco à reputação e barreira de proteção:** criar equipes de comunicação treinadas em procedimentos de prevenção específicos para gerenciar completamente os ciber-riscos, mantendo-se sempre disponível. Será necessário usar ferramentas digitais de monitoramento e gerenciamento que possam reduzir significativamente a distância entre o tempo humano e o tempo da máquina ao gerenciar alertas, estabelecer estratégias e implementar táticas de gerenciamento de crises.
- **Redução do tempo:** o gerenciamento da cibersegurança exigirá a inclusão de novas ferramentas digitais específicas combinada à perspectiva fornecida por analistas de dados especializados das áreas de comunicação dos departamentos jurídico, financeiro e de reputação.

Em suma, as grandes empresas enfrentam grandes desafios referentes à cibersegurança. As empresas devem fazer grandes esforços para adaptar seus materiais, procedimentos e metodologias às exigências dos novos regulamentos, sem ignorar o fato de que a gestão de ciberataques será um elemento importante na gestão da reputação da empresa, para não abalar a confiança. Portanto, o paradigma de segurança estará ligado à transformação digital holística da empresa, à adaptabilidade das organizações, à nova comunicação e à dinâmica do comportamento social digital.

Figura 3. Cinco tendências da segurança em empresas da Espanha



Fuente: PwC, *The Global State of Information Security Survey 2017.*

Luis Serrano é Diretor da Área de Crise da LLORENTE & CUENCA. Luis é formado em Jornalismo e um dos principais especialistas na Espanha no campo de gestão da comunicação de emergências e catástrofes, e no desenvolvimento de planos de ação para crises em redes sociais. Foi assessor de imprensa do Centro de Emergência de Madri 112 por 17 anos, onde participou ativamente na gestão de situações críticas, como os ataques de 11M em Madri. Ele interveio em mais de 100 acidentes de trabalho, acidentes com múltiplas vítimas, acidentes em áreas de lazer, crises de saúde, etc. Seu livro *11 M and other catastrophes. Managing communication in emergencies* é o resultado de todas essas experiências. Ele também tem vasta experiência de ensino no campo de emergências e gestão de crises. É docente do Curso de Mestrado em Emergências da CEU-TASSICA e do Programa de Mestrado em Incêndio da Universidade de Lleida. Mestrado em Comunicação Política da Universidade Camilo José Cela, Mestrado em Segurança e Emergências de da Fundação Ortega y Gasset e Universidade Rey Juan Carlos, Mestrado em Emergências da Universidade Murcial-Alebat. Também trabalhou como docente por 12 anos na Escola Nacional de Proteção Civil da Espanha. Como jornalista, passou sete anos trabalhando para os serviços de informação da Onda Cero.

lserrano@llorenteycuenca.com

Natalia Sara é Gerente da Área de Crise da LLORENTE & CUENCA. Natalia é formada em Ciência da Informação pela Universidade de Navarra, e tem mestrado em gestão e liderança de recursos humanos e mestrado em marketing, internet e novas tecnologias pela ESIC Business & Marketing School. Ela tem 25 anos de experiência no campo de comunicação, dos quais os 15 últimos como consultora de assuntos públicos e crise, e inicialmente como jornalista para grandes veículos da mídia nacional, como Expansión o Actualidad Económica. Ela é especializada em comunicação de crise e reputação e tem vasta experiência no desenvolvimento de protocolos, manuais de crise e desempenho estratégico para evitar riscos potenciais e gerenciar situações adversas para marcas, pessoas e organizações. Ela treina gestores e profissionais de comunicação e gestão de reputação digital; é professora da Escola de Jornalismo e Comunicação Unidad Editorial, em Comunicação Corporativa Digital e Gestão de Crises Online, e da Foro Europeo Business School. É autora da seção sobre gestão de crises do livro *Political Consultancy*, publicado pelo Centro Internacional de Governo e Marketing Político (CIgMAP) da Universidade Camilo José Cela (UCJC).

nsara@llorenteycuenca.com

d+i desenvolvendo ideias
LLORENTE & CUENCA

Desenvolvendo Ideias é o Departamento de Liderança através do Conhecimento da LLORENTE & CUENCA.

Porque estamos testemunhando um novo modelo macroeconômico e social. E a comunicação não fica atrás. Avança.

Desenvolvendo Ideias é uma combinação global de relacionamento e troca de conhecimentos que identifica, se concentra e transmite os novos paradigmas da comunicação a partir de uma posição independente.

Porque a realidade não é preta ou branca existe **Desenvolvendo Ideias** na LLORENTE & CUENCA

www.desarrollando-ideas.com
www.revista-uno.com.br