Compreender a DORA: Um guia para o Ato de Resiliência Operacional Digital

Barracuda

O Digital Operational Resilience Act (DORA) é um regulamento da União Europeia (UE) que entra em vigor a 17 de janeiro de 2025 e visa reforçar a resiliência das instituições financeiras em matéria de cibersegurança.

A legislação assinala uma mudança fundamental na forma como o público e os reguladores veem a cibersegurança e a transparência corporativa. Reconhece a necessidade de as empresas levarem a defesa a sério e que ser aberto sobre as violações torna a vida mais segura para todos.

O DORA é um reconhecimento da crescente dependência do setor dos serviços financeiros em relação à infraestrutura digital e da importância de garantir a segurança dessa infraestrutura. Representa as melhores práticas, exigindo que as empresas estabeleçam práticas resilientes e comuniquem violações e falhas.

A legislação reflete o entendimento de que um ataque bem-sucedido à infraestrutura financeira digital pode causar danos em toda a sociedade. Os efeitos podem ser duradouros, exigindo tempo e dinheiro para recuperação e reparação. Os cibercriminosos e os agentes patrocinados pelo Estado têm acesso a ferramentas de ataque cada vez mais sofisticadas e automatizadas. A segurança digital já não é um extra opcional, mas sim uma obrigação para estar no mercado.

Este eBook oferece uma visão geral do DORA, fontes para saber mais e as melhores práticas necessárias para conformidade. Também identifica os recursos da Barracuda que o podem ajudar a preparar-se para a implementação.

A quem se aplica o DORA?

O DORA aplica-se à maioria das instituições financeiras, incluindo:

- Bancos, companhias de seguros, firmas de investimento e instituições de crédito
- Prestadores de serviços de pagamento e FinTechs
- Gestores de ativos e plataformas de negociação

O DORA abrange essencialmente qualquer entidade envolvida no setor financeiro que utilize serviços de tecnologia e comunicação, bem como os seus fornecedores de serviços críticos de TIC a terceiros. Abrange não só as empresas da UE, mas também todas as empresas do mundo com atividades ou clientes no território. Embora as empresas britânicas que não têm clientes na UE não precisem de cumprir o DORA, espera-se que o governo do Reino Unido crie o seu próprio quadro regulamentar que, provavelmente, será muito semelhante à regulamentação europeia. Mas, para além da conformidade, garantir que a sua organização está em conformidade com as recomendações do DORA significa que está a seguir as melhores práticas modernas.

Quais são os cinco componentes chave dos regulamentos DORA?

O objetivo geral do DORA é reforçar a resiliência operacional das instituições financeiras aos ciberataques e harmonizar as regras em toda a UE. O regulamento tem cinco componentes principais:

Gestão de Risco: As instituições financeiras devem ter procedimentos robustos de gestão do risco de TI em vigor. Isto inclui procedimentos para identificar, avaliar e mitigar riscos potenciais relacionados com os seus sistemas de TI, sistemas cloud e redes da cadeia de abastecimento.

Testar a resiliência: A DORA reconhece que nenhuma medida de segurança é fiável se não for testada. As instituições financeiras devem dispor de um plano adequado de resposta a incidentes e de pessoal que compreenda o seu funcionamento. Estas instituições devem testar periodicamente a robustez da sua infraestrutura digital contra perturbações operacionais, por exemplo, através de testes de penetração, testes de resistência e avaliações de vulnerabilidade.

Relatórios de incidentes: Realizar avaliações de risco abrangentes e implementar políticas robustas relativas à segurança do sistema de informação. Isto irá garantir uma abordagem proativa para identificar e mitigar quaisquer ameaças potenciais. Estabeleça processos de resposta a incidentes, realize simulações e treine a sua equipa para estar preparada.

Gestão de Riscos de Terceiros: DORA também reconhece o perigo dos ataques à cadeia de fornecimento. Exige que as instituições financeiras monitorizem os provedores de serviços terceirizados, especialmente aqueles como as empresas de computação em cloud. As instituições devem firmar acordos escritos com seus fornecedores que abordem os tópicos indicados no Artigo 30 da DORA, como uma descrição escrita de todos os serviços fornecidos e, quando aplicável, compromissos de nível de serviço.

Partilha de Informações: O regulamento visa harmonizar as obrigações de comunicação dentro da UE e reforçar a postura de segurança de todo o setor, incentivando uma melhor cooperação e partilha de informações entre empresas. Isso significa um dever de relatar incidentes rapidamente após a sua ocorrência. No passado, isso acontecia de forma ad hoc e não transparente.

Conformidade e aplicação

Pode parecer que DORA não representa um desvio radical das melhores práticas estabelecidas. Esta é uma suposição justa. O que é diferente com o DORA, no entanto, é que o regulamento exigirá que as instituições provem que estão a fazer o que deveriam estar a fazer. Não existe uma certificação única ou um teste de conformidade, mas o DORA irá acrescentar um encargo de governação e documentação a muitas empresas. A aplicação da legislação será da responsabilidade dos três reguladores financeiros atuais da UE - as Autoridades Europeias de Supervisão.

Penalidades

As entidades reguladoras têm a discricionariedade de aplicar sanções às organizações que não cumpram o regulamento. Os Estados-Membros também têm a discricionariedade para impor penalidades criminosas.

Quais são os primeiros passos para a conformidade com a DORA?

A primeira tarefa é determinar se o DORA se aplicará diretamente à sua empresa. Como referido anteriormente, mesmo que não se aplique diretamente, as instituições financeiras devem considerar o conjunto razoável de melhores práticas de cibersegurança no DORA. Quer os seus planos de crescimento envolvam a expansão para a UE ou a realização de negócios com instituições financeiras que operam na UE, é aconselhável trabalhar para estar em conformidade agora. Se precisar de estar totalmente em conformidade até janeiro, terá de agir rapidamente e, quando necessário, procurar ajuda externa. Se presta serviços a empresas da UE que operam em serviços financeiros, deve envolver-se de perto com elas para alinhar as suas estratégias.

O seu segundo passo é completar uma análise de lacunas para medir o grau de maturidade da sua postura de cibersegurança e até que ponto os seus sistemas reflectem os exigidos pelo regulamento. Uma vez concluído, pode começar a preencher as lacunas e a pôr em prática as pessoas, os processos e a tecnologia necessários.

Saiba mais

A Autoridade Europeia dos Seguros e Pensões Complementares de Reforma disponibiliza um bom guia centrado nas empresas para DORA. E se pretender aprofundar o assunto, podeconsultar a legislaçãoatual (PDF de 75 páginas).

A Barracuda Networks pode ajudar a sua organização a cumprir todos os cinco componentes principais do DORA. O nosso conjunto abrangente de ferramentas de Cibersegurança pode fortalecer a sua postura de segurança em todas as áreas, de Email a aplicação web e segurança de rede.

Temos uma riqueza de recursos online para o ajudar a lidar com o DORA, incluindo o uso de XDR para melhorar a sua deteção e resposta à gestão de ameaças, e como obter o conselho para apoiar estratégias de cibersegurança.

Também podemos ajudar aperfeiçoar a sua resposta a incidentes. Finalmente, o Barracuda Security Insights pode ajudar a fornecer a inteligência ativa de que precisa para potenciar a sua análise de risco.

Sobre a Barracuda

A Barracuda é uma empresa global de cibersegurança líder, que oferece proteção completa contra ameaças complexas para empresas de todos os tamanhos. A nossa plataforma BarracudaONE, potenciada por IA, protege e-mail, dados, aplicações e redes com soluções inovadoras, XDR gerido e um painel de controlo centralizado para maximizar a proteção e reforçar a resiliência cibernética. Confiada por centenas de milhares de profissionais de TI e provedores de serviços geridos em todo o mundo, a Barracuda oferece defesas poderosas que são fáceis de comprar, implantar e usar. Para mais informações, visite pt.barracuda.com.