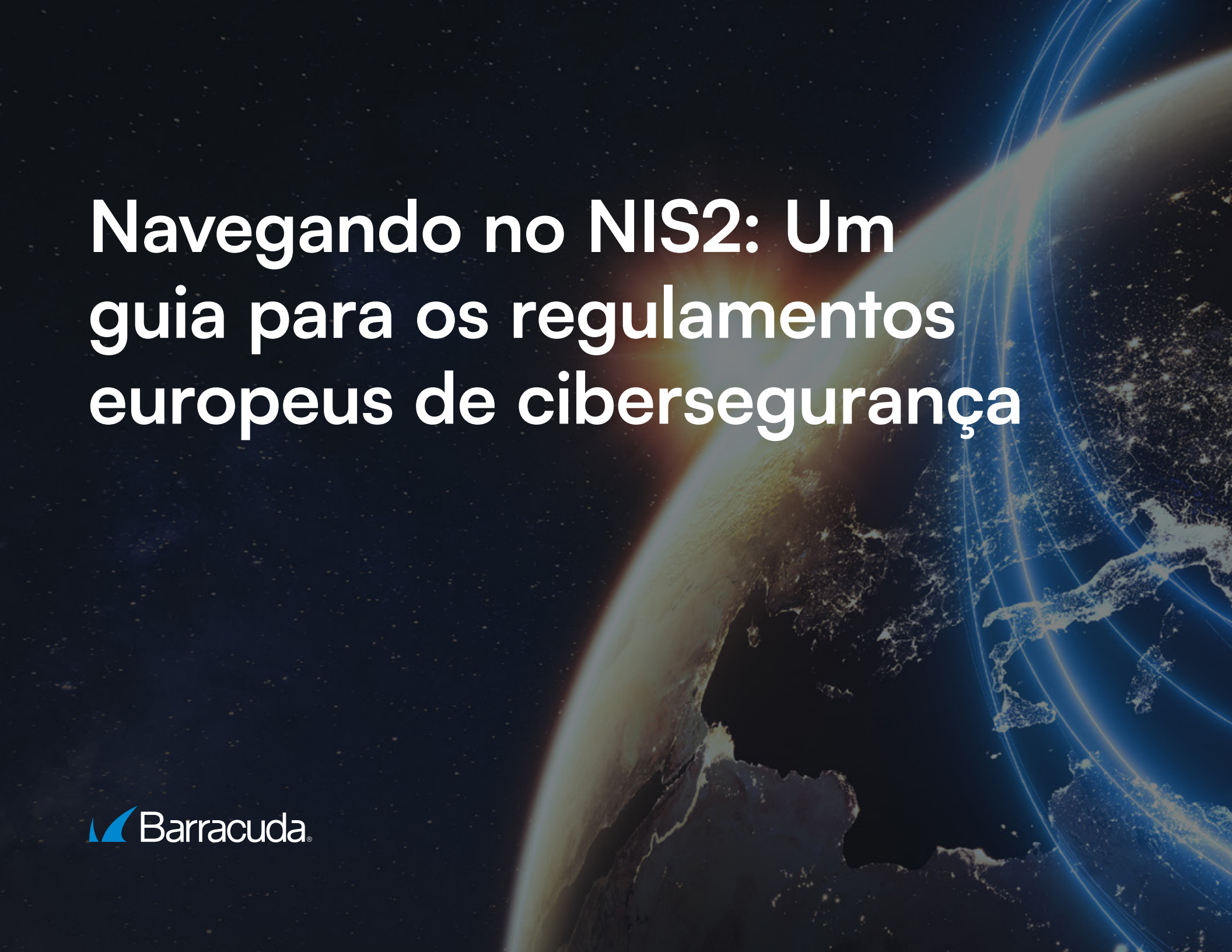
Navegando no NIS2: Um guia para os regulamentos europeus de cibersegurança



Barracuda

A evolução das regulamentações de cibersegurança na Europa

A mudança no papel das regulamentações de cibersegurança na Europa reflete o crescente reconhecimento da ameaça crescente que as violações e os cibercriminosos representam para as empresas e organizações individuais — e para a sociedade em geral. Porque a nossa sociedade é agora composta por organizações cada vez mais interligadas, qualquer ataque pode ter consequências amplas e inesperadas.

Alterações recentes às regulamentações da União Europeia (UE), conhecidas como NIS2 (Diretiva de Segurança de Redes e Informação 2), também mencionam o impacto da COVID-19 nas práticas de trabalho. Com mais de nós a trabalhar em casa desde a pandemia, a superfície de ameaça potencial aumenta, tal como a nossa dependência das redes para realizar o trabalho — e o resto das nossas vidas —.

Mas também reflete a crescente maturidade da regulamentação da cibersegurança. Enquanto as organizações trabalham para se manterem seguras, reconhece-se também que precisamos de leis unificadas e de normas mínimas para nos mantermos a todos seguros.

O primeiro passo nesta jornada foi dado em 2016, com a Diretiva de Segurança de Redes e Informação, ou NIS1. Isto estabeleceu padrões básicos de cibersegurança para organizações que operam em setores críticos, incluindo água, infraestruturas digitais, banca, saúde e transportes. O NIS2 expande estes padrões, abrangendo um conjunto muito mais amplo de setores.

Dito isto, é importante notar que a NIS2 é uma diretiva, não uma lei — precisa ser transposta para a legislação nacional pelos Estados-Membros, o que alguns já fizeram. A NIS2 está agora em vigor, com vários países, incluindo a Bélgica, a Croácia e a Itália, a incorporá-la na legislação local e outros em processo de adoção.

A NIS2 está a transformar e a informar a regulamentação, tanto na UE como fora dela. Este é outro dos principais impulsionadores da legislação de cibersegurança. Não opera num único Estado-nação. As empresas que interagem com cidadãos ou outras empresas na UE devem seguir as mesmas regras. Estamos a caminhar para um mundo em que as normas de cibersegurança são partilhadas por todos os países, e as empresas serão obrigadas a cumpri-las para poderem fazer negócios e para garantir aos clientes que estão a aplicar a regulamentação.

Note-se também que o Governo do Reino Unido se comprometeu a não adotar a NIS2 na legislação nacional, mas sim a alargar a NIS1 em conformidade com outros regulamentos, como o Projeto de Lei de Cibersegurança e Resiliência. Mas olhando para o que é realmente sugerido, parece que o Reino Unido e a UE estão a caminhar na mesma direção com as alterações que estão a ser feitas — embora a legislação proposta no Reino Unido prometa ser menos onerosa. Também não é claro quando é que o Governo do Reino Unido vai encontrar tempo parlamentar para efetuar estas alterações. Na realidade, a maioria das organizações que trabalham ou efetuam transações comerciais com a UE escolherá provavelmente um conjunto de regras a cumprir em vez de dois.

Os fundamentos do NIS2

Quem:

Aplica-se em toda a UE, mas as empresas de qualquer parte do mundo que façam negócios ou prestem serviços a empresas ou organizações na UE também terão de seguir as práticas NIS2.

Alarga as regras das grandes organizações que lidam com infraestruturas críticas às empresas mais pequenas e às definidas pela UE como Essentials.

Regras alargadas às empresas com mais de 50 trabalhadores em determinados sectores.

Energia, transportes, banca, saúde, infraestruturas digitais, fornecedores de computação em cloud, prestadores de serviços de segurança geridos, Gestão de resíduos, produtores de alimentos, grande parte da indústria transformadora, motores de pesquisa e organismos de investigação estão todos incluídos.

O que:

Estabelece regras para que os países estejam preparados para incidentes de cibersegurança e incentiva a cooperação transfronteiriça.

Os Estados-Membros deveriam transpor a diretiva para o direito nacional até outubro de 2024. Vários o fizeram, enquanto outros estão em várias fases de adoção. Verifique o estado atual da transposição.

Notificação obrigatória de incidentes.

Como:

A cibersegurança é uma responsabilidade clara da gestão sénior — e a NIS2 fá-lo tornando-os pessoalmente responsáveis pelas falhas.

A diretiva, e as suas equivalentes nas legislações nacionais, abrange uma seleção mais vasta de empresas e organizações — não apenas infraestruturas vitais, mas também as definidas pela UE como Essentials.

Define o dever de dar um alerta antecipado de incidentes no prazo de 24 horas, fornecer uma notificação mais detalhada no prazo de 72 horas e um relatório detalhado no prazo de um mês. Isto visa criar dois efeitos benéficos. Em primeiro lugar, para incentivar a conformidade sob ameaça de publicidade indesejada e, em segundo lugar, para fornecer insights acionáveis a outras organizações que provavelmente serão alvos de ataques semelhantes.

NIS2 essentials: O que precisa fazer para estar em conformidade

Deve notar-se que o NIS2 é muito semelhante a qualquer manual de best practice para uma boa higiene geral da Cibersegurança, embora seja acompanhado de sanções financeiras severas em caso de incumprimento. As sanções previstas na NIS2 são severas, com coimas que podem atingir 10 milhões de euros ou 2% do volume de negócios anual global, consoante o montante mais elevado.

A conformidade com a diretiva e a proteção para o negócio significam determinar o que é necessário para proteger dispositivos, ativos e dados. Isto significa segurança física, cibersegurança e pessoal treinado para operar de forma segura. Além de implementar tais medidas, as organizações devem também demonstrar que têm uma estratégia eficaz de gestão de riscos em vigor. Isso inclui provar o que fez — que avaliou o estado das suas redes, sistemas de TI e competências humanas, e agiu onde apropriado.

Tem de demonstrar que tem um plano em vigor para o tratamento de incidentes se o pior acontecer. Terá de demonstrar que avaliou a segurança da cadeia de abastecimento, a gestão e divulgação de vulnerabilidades — e que tem uma estratégia em vigor para a utilização de criptografia e, quando apropriado, encriptação.

O NIS2 reconhece as certificações de cibersegurança da UE de produtos e soluções para ajudar a aliviar o ónus da conformidade para as empresas. Se a sua organização já está em conformidade com a norma ISO 27001, está no bom caminho para satisfazer a norma NIS2.

Mas, como sempre, a conformidade não deve ser vista apenas como um fim em si mesma. A conformidade pode ser uma ótima maneira de conquistar corações e mentes e obter amplo apoio para estratégias de cibersegurança que, de qualquer forma, devem fazer parte do pensamento empresarial em todos os níveis. A conformidade não significa proteção completa, mas certamente não o colocará em mais risco.

A maioria das organizações compreende agora que precisa de planear para incidentes — mesmo que espere que estes nunca ocorram e trabalhe arduamente para evitar que aconteçam.

Da mesma forma, a atitude mudou em relação ao relato de incidentes. Mais pessoas aceitam agora os benefícios e o papel que o relato de incidentes desempenha para manter outras organizações mais seguras, e reconhecem que até fornece um modelo para a defesa contra novos ataques.

Best Practice para Conformidade e segurança: Compreender a diferença

Os profissionais de cibersegurança têm de compreender a diferença entre conseguir a conformidade e conseguir a melhor proteção possível. Estas não são a mesma coisa. As organizações precisam de demonstrar a conformidade — precisa de ser capaz de mostrar, com provas, a terceiros que o que fez é tão seguro quanto possível. É como mostrar à sua companhia de seguros que tem as fechaduras e os alarmes certos para proteger o seu armazém. Tudo isso é necessário, mas precisa de ir além disso para estar verdadeiramente seguro.

Aqui estão 13 elementos a considerar na sua jornada para a conformidade com o NIS2:

Política de segurança de rede: Estabeleça uma política sobre a segurança da rede e dos sistemas de informação que defina as funções e responsabilidades dos vários departamentos da empresa com um processo para monitorizar a conformidade.

Avaliação de risco: Estabelecer e implementar uma política de tratamento de incidentes que defina as funções, responsabilidades e procedimentos para detetar, analisar, conter ou responder, recuperar, documentar e relatar incidentes em tempo hábil.

Continuidade de negócios e gestão de crises: Desenvolver e manter um plano de continuidade de negócios, gestão de crises e recuperação de desastres a aplicar no caso de incidentes de cibersegurança e outras crises que inclua planos de backup para recursos críticos, incluindo pessoal. Treine o pessoal aplicável nestes documentos e conduza crises simuladas regulares para garantir que todos saibam e possam desempenhar as suas funções.

Política de segurança da cadeia de abastecimento: Criar e implementar uma política de segurança da cadeia de abastecimento que inclua uma avaliação das práticas de segurança dos potenciais fornecedores como parte do processo de contratação.

Compreender o uso de fornecedores de tecnologias da informação e comunicação (TIC): Mapeie os seus fornecedores de TIC, o que eles fazem, quais são críticos para as suas operações, e os padrões de segurança que esses fornecedores devem cumprir. Mantenha um diretório de fornecedores críticos, incluindo informações de contacto. Desenvolva um processo para avaliar a conformidade do fornecedor com os padrões de segurança.

Avaliação do processo de risco cibernético: Crie um processo no qual avalia a eficácia dos seus procedimentos de risco cibernético e realiza essa avaliação periodicamente.

Formação em segurança: Fornecer formação em cibersegurança e promover práticas básicas de ciber-higiene entre os colaboradores para fomentar uma cultura de segurança e sensibilização.

Criptografia: Desenvolver e impor o uso correto de criptografia e encriptação para garantir a confidencialidade e integridade de dados sensíveis.

Segurança de RH: Implementar políticas e procedimentos que regem o comportamento dos funcionários em relação à higiene da segurança cibernética. Utilize procedimentos apropriados de triagem de antecedentes em conformidade com a lei aplicável ao contratar pessoal. Crie um processo padrão para revogar todo o acesso aos ativos de tecnologia da informação da empresa e informações da empresa quando os funcionários deixarem a empresa.

Controle de acesso: Implementar procedimentos de segurança para funcionários com acesso a dados confidenciais. Use a autenticação multifator (MFA) e a avaliação contínua de Zero Trust e, quando apropriado, criptografe as comunicações de emergência internas para melhorar as medidas de segurança.

Classificar ativos da empresa: Configurar um sistema para classificar as informações da empresa, como informações confidenciais de negócios e informações sensíveis (por exemplo, informações de saúde, números de identificação governamental, cartões de crédito, etc.).

Segurança ambiental e física: Avalie o suporte à infraestrutura crítica para os locais da empresa, como sistemas de comunicações e energia, e, quando possível, implemente processos de backup. Proteja as localizações físicas de ameaças externas, incluindo controlos de acesso físico.

Pessoas e processos em primeiro lugar, tecnologia em segundo

Os fornecedores são frequentemente culpados de venderem soluções primeiro. Mas, na realidade, tem de começar por implementar os processos, procedimentos e pessoas corretos e, em seguida, pensar na tecnologia para apoiar e reforçar estas capacidades. As equipas de segurança consideram frequentemente os seres humanos como o elo mais fraco em vez de a sua primeira linha de defesa.

A formação do seu pessoal e o reforço das suas competências em matéria de segurança é um passo vital, reconhecido na diretiva NIS2.

Qualquer alteração regulamentar é uma boa oportunidade para revisitar o básico e avaliar o que está a fazer bem e onde há espaço para melhorias.

Precisa de bons controlos de acesso e gestão de identidade. Precisa de proteção de e-mail — que continua a ser o vetor e o ponto de partida mais comum para um ataque. Também precisa de proteção de rede e firewalls.

Mas também precisa de alguns sistemas de segurança mais inteligentes a trabalhar para si. Analisar o comportamento da rede e das aplicações é cada vez mais importante num mundo em que identificar o 'limite' de qualquer rede é cada vez mais difícil. Isto também pode ajudar a protegê-lo contra ataques à cadeia de abastecimento.

A Barracuda pode ajudá-lo a cumprir os requisitos NIS2 — e a melhorar a sua postura de segurança geral — com proteção de aplicações, proteção de rede e proteção de e-mail. Podemos até fornecer XDR gerido para supervisionar tudo isto.

Sobre a Barracuda

Barracuda est une entreprise de cybersécurité leader sur son marché, offrant aux entreprises de toutes tailles une protection complète face aux menaces complexes. Notre plateforme BarracudaONE, propulsée par l'IA, sécurise les emails, les données, les applications et les réseaux grâce à des solutions innovantes, un XDR managé et un tableau de bord centralisé afin de maximiser la protection et renforcer la résilience cyber. Des centaines de milliers d'organisations et de fournisseurs de services managés (MSP) du monde entier nous font confiance pour les protéger et les accompagner, avec des solutions faciles à acquérir, déployer et utiliser. Pour plus d'informations, visitez pt.barracuda.com.

Barracuda