OBJECT FIRST

Whitepaper

Diretiva NIS2

Fatos essenciais e como cumprir

Cartilha do NIS2

Conforme os ataques cibernéticos tornaram-se mais frequentes e sofisticados, os governos e agências internacionais estão propondo regulamentos novos e renovados para reforçar a resiliência em setores críticos. Na União Europeia (EU), isso foi colocado em prática com a Diretiva de segurança de redes e informações 2 (NIS2). As organizações de toda a UE devem tomar medidas para cumprir seus requisitos e evitar riscos regulatórios e de reputação.

Se você trabalha na área de TI na UE, é fundamental compreender a NIS2 para proteger sua infraestrutura e manter a confiança. Esta cartilha rápida analisa os principais elementos da diretiva para ajudar você a estar em conformidade com ela e sempre à frente dos atacantes.

O que é NIS2?

A Diretiva de segurança de redes e informações 2 (NIS2) visa reforçar a cibersegurança nos estados-membros da UE e em todas as entidades que fazem negócios com eles. Trata-se de uma resposta às crescentes ameaças associadas à digitalização e ao aumento dos ataques cibernéticos.

A NIS2 amplia o escopo da Diretiva NIS original com mais setores e tipos de entidades que enquadram-se em sua jurisdição, inclusive aquelas cuja função é considerada "essencial" e "importante" no mercado interno da UE. Ela introduz requisitos mais significativos, como a apuração completa de incidentes, práticas de gerenciamento de riscos, medidas de responsabilização corporativa e estratégias de continuidade dos negócios.

Sou essencial ou importante?

A NIS2 categoriza as organizações empresariais em dois grupos: "essenciais" e "importantes". Seu enquadramento nessa organização ajudará a entender como a NIS2 afetará sua organização.

Riscos de não conformidade

A Diretiva NIS2 inclui sanções significativas por não conformidade, incluindo multas substanciais e possível litígio. Os estados-membros da UE foram obrigados a incluir a NIS2 na legislação nacional até 17 de outubro de 2024. Embora nem todos os países tenham cumprido o prazo, todos estão a trabalhar ativamente para implementar a diretiva; vários já fazem cumprir a legislação nacional e outros estão em estágio avançado de adoção.

Deve compreender a diretiva de forma proativa, identificar os impactos na sua organização e estabelecer um plano para atingir a conformidade.

Neste momento, é provável que você esteja se perguntando: "Como isso me afeta?". Mas, primeiro deve entender quem é "você" e se a NIS2 afeta a sua organização.

Entidades essenciais

A NIS2 identifica setores cruciais, como os de transportes, serviços financeiros, cuidados de saúde e empresas de serviços públicos (inclusive fornecedores de energia) como "entidades essenciais", enfatizando sua importância para o bem-estar social e econômico. Ela aumenta suas obrigações de conformidade, especialmente a exigência de notificação de incidentes no prazo de 24 horas. Os requisitos tornaram-se significativamente mais rígidos que os da diretiva anterior. Além disso, introduz multas pesadas e consequências graves pelo não cumprimento, enfatizando os riscos maiores e o cenário regulamentar mais rigoroso que essas entidades enfrentam atualmente.

Será uma entidade essencial se a sua empresa tiver mais de 250 funcionários, um volume de negócios anual de € 50 milhões e se enquadrar em alguma destas categorias:

- Infraestrutura digital
- Energia
- Finanças
- Saúde
- Administração pública
- Espaço
- Transportes
- Fornecimento de água (potável e residual)

Entidades importantes

A NIS2 introduz uma nova classificação de entidades "importantes", ampliando o escopo da diretiva para englobar pela primeira vez setores como os serviços postais, a gestão de resíduos e a manufatura. Com essa expansão, esses setores precisam avaliar e melhorar suas medidas de cibersegurança para estar em conformidade com a NIS2. Embora as obrigações e sanções das entidades "importantes" sejam menos severas em caso de não conformidade do que as das contrapartes "essenciais", não se pode subestimar o desafio de cumprir esses requisitos.

Será uma entidade "importante" se a sua empresa tiver mais de 50 funcionário e um volume de negócios anual de € 10 milhões e se enquadrar em uma destas categorias (inclui também as categorias listadas como essenciais):

- Produtos químicos
- Alimentos
- Manufatura
- Serviços postais
- Pesquisa
- Gestão de resíduos

Entidades essenciais

Se a sua empresa se enquadra nas categorias "essencial" ou "importante" listadas, o próximo passo é compreender o que a NIS2 significa para a sua organização e de que forma o pode afetar.

Introdução

A Diretiva NIS2 enfatiza uma estratégia de cibersegurança meticulosa nas organizações. Embora seja uma estrutura regulamentar muito detalhada, e recomendamos que as organizações afetadas nos estados-membros se empenhem em ler os artigos, separamos alguns itens importantes para ajudar a começar sua avaliação, iniciando com dez medidas de cibersegurança mínimas destacadas na diretiva.

As dez medidas de gerenciamento de riscos de cibersegurança

Uma das seções mais importantes da diretiva é o Artigo 21, que lista dez medidas de gerenciamento de riscos de cibersegurança. Os estados-membros devem assegurar que as entidades "essenciais" e "importantes" implementem medidas técnicas, operacionais e organizacionais adequadas para gerenciar os riscos à segurança dos sistemas de rede e informações usados em suas operações ou serviços. Essas medidas devem evitar ou minimizar o impacto de incidentes nos destinatários dos serviços. Elas devem considerar a tecnologia mais recente, as normas relevantes e os custos, além de garantir que o nível de segurança seja apropriado ao nível de risco. Ao avaliar a proporcionalidade das medidas de segurança, as organizações têm de considerar sua exposição ao risco, a dimensão e o potencial impacto dos incidentes. Isto inclui avaliar a gravidade e probabilidade de incidentes e os respetivos efeitos sociais e económicos.

A Diretiva NIS2 lista dez medidas de cibersegurança que todas as entidades qualificadas devem implementar:

1. Tratamento de incidentes
2. Políticas de análise de riscos e segurança dos sistemas de informações
3. Processos de continuidade dos negócios, como gerenciamento do backup, recuperação de desastres e gerenciamento de crises
4. Segurança da cadeia de fornecimento, incluindo aspectos relacionados à segurança relativos aos relacionamentos entre cada entidade e seus fornecedores ou prestadores de serviços diretos
5. Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informações, incluindo o tratamento e a divulgação de vulnerabilidades
6. Práticas básicas de higiene cibernética e treinamento em cibersegurança
7. Segurança dos recursos humanos, políticas de controle de acesso e gerenciamento de ativos
8. Políticas e procedimentos relacionados ao uso de codificação e, quando apropriado, da criptografia
9. Soluções de autenticação multifator ou de autenticação contínua, comunicações seguras por voz, vídeo e texto e sistemas seguros de comunicação de emergência na entidade, quando apropriado.
10. Políticas e procedimentos para avaliar a eficácia das medidas de gerenciamento de riscos de cibersegurança

Dever de notificação

Um tema recorrente em toda a Diretiva NIS2 é a importância da notificação. As entidades "essenciais" são obrigadas a estabelecer procedimentos para a rápida notificação de incidentes de cibersegurança significativos, com prazos específicos para a notificação, incluindo um sistema preliminar de "alerta rápido" de 24 horas.
A NIS2 também destaca a importância da responsabilidade corporativa, exigindo que a administração se envolva ativamente com e compreenda as iniciativas de cibersegurança da organização. Os gestores podem ser penalizados por violações de segurança, podendo ser responsabilizados e mesmo proibidos temporariamente de ocupar cargos de direção.

Sanções

As novas regras da Diretiva NIS2 são muito mais exigentes do que anteriormente, introduzindo multas mais elevadas ou totalmente novas, em alguns casos.

No entanto, os países da União podem decidir aplicar multas ainda mais elevadas. As empresas consideradas "essenciais" devem estar preparadas para enfrentar multas de até € 10 milhões ou 2% de sua receita anual global do último ano, o que for maior. As empresas consideradas "importantes" podem receber multas de até € 7 milhões ou 1,4% de sua receita global do ano anterior, novamente o que for maior.

Espere, tem mais

Estas três seções apresentam diversas expectativas da Diretiva NIS2; no entanto, não são completas. Incentivamos todas as empresas que operam na União Europeia a analisar toda a diretiva e seus requisitos com as suas equipes para compreender plenamente as expectativas e ramificações desta legislação de grande dimensão.

Como a Object First pode ajudar

A NIS2 representa uma evolução extremamente importante na regulamentação da segurança e pode ser um impulso significativo para garantir a conformidade no data center de entidades “importantes” e “essenciais”. Além de redigir esta cartilha, pensamos em estender algumas das nossas recomendações para ajudar a garantir que possa atingir suas metas da NIS2 de maneira eficiente.

Zero Trust Data Resilience (Resiliência de dados de Zero Trust)

A seção 89 da introdução da Diretiva NIS2 menciona as organizações que adotam o princípio Zero Trust (confiança zero) para ajudar a melhorar sua postura de segurança global. Zero Trust é um conjunto essencial de princípios para garantir a segurança das aplicações e infraestruturas de produção. No entanto, não considera o software de backup e o armazenamento de backup como parte de seu modelo de maturidade global.

A Veeam e a Numberline publicaram recentemente uma pesquisa sobre Zero Trust Data Resilience (ZTDR) (Resiliência de dados de Zero Trust). Trata-se de uma abordagem abrangente de proteção de dados que expande os princípios de segurança Zero Trust para o ambiente de backup da organização. Ela introduz elementos críticos, como a separação do software de backup e do armazenamento de backup, várias zonas de resiliência e o armazenamento de backup imutável e criptografado. Essa abordagem minimiza o risco, reforça a proteção de dados e intensifica a postura de segurança da organização. É fundamental que as organizações entendam a ZTDR, pois ela oferece uma estrutura robusta para proteger os dados de ameaças cibernéticas, especialmente ataques de ransomware e exfiltração de dados. Ela representa uma alternativa mais segura que os modelos de segurança tradicionais com relação à proteção de dados e deve fazer parte da lista de verificação de todos os administradores para a preparação para a Diretiva NIS2. Para obter mais informações sobre a ZTDR, leia nosso whitepaper.

Armazenamento de dados de backup imutável

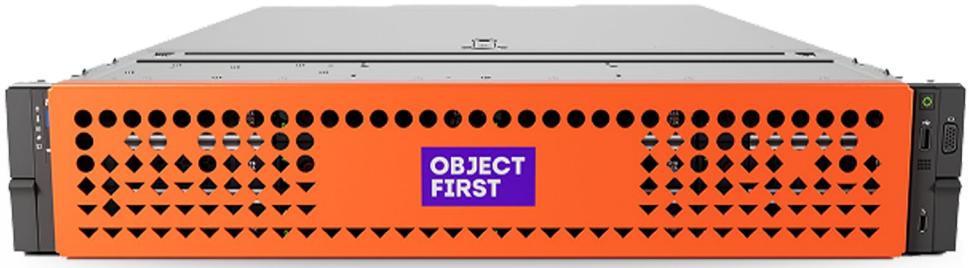
Surpreendentemente, a palavra “imutabilidade” não é mencionada na Diretiva NIS2. A parte mais importante da proteção de dados é a capacidade de recuperação e, com o armazenamento imutável, a probabilidade de recuperação é muito maior. Atualmente, a maioria dos ataques visa primeiro a infraestrutura de backup para eliminar a possibilidade de recuperação e garantir o pagamento do resgate.

As medidas de cibersegurança do Artigo 21 da NIS2 mencionam diretamente os requisitos de proteção de dados, a higiene cibernética e a criptografia. Ainda assim, é possível violar e destruir tudo isso. Por outro lado, uma meta de armazenamento imutável em conformidade com as melhores práticas de ZTDR, como o acesso zero à raiz, uma arquitetura inerentemente segmentada do software de backup e um armazenamento que utilize o bloqueio de objetos S3 em modo de conformidade, ajudará a aumentar a resiliência em face de um ataque. No entanto, para garantir a recuperação, é necessária a Imutabilidade Absoluta. Ninguém, nem mesmo o administrador com mais privilégios ou atacante com acesso ao armazenamento de backup, pode modificar ou eliminar dados.

Como atingir os objetivos de tempo de recuperação

A diretiva inclui várias declarações sobre a importância de uma estratégia de recuperação, incluindo um plano de recuperação reativo e testes de simulações de recuperação antes da ocorrência de um ataque cibernético. Recomendamos que todas as organizações afetadas pela legislação NIS2 se empenhem em avaliar seus ambientes de proteção de dados atuais e executar cenários de recuperação de teste para avaliar melhor seus verdadeiros objetivos de ponto de recuperação (RPO) e objetivos de tempo de recuperação (RTO). Compreender até que ponto é necessário recuar na recuperação, em conjunto com o tempo que será necessário para recuperar os dados, é uma parte crucial da capacidade de resposta exigida pela NIS2.

Conheça o Ootbi (Imutabilidade Out-of-the-box)



A Object First procura ajudar todos os clientes da Veeam na UE a garantir que seu armazenamento de backup exceda os padrões da NIS2. Por isso, a Object First criou o Ootbi, o melhor armazenamento para a Veeam. À prova de ransomware e com imutabilidade out-of-the-box, o Ootbi da Object First oferece armazenamento de backup seguro, simples e eficiente absolutamente imutável. Com a melhor defesa contra ransomware, você e a sua organização tornam-se Simplesmente Resilientes.

A Object First foi criada com base nas práticas recomendadas de Zero Trust e foi testada por terceiros para ser segura, é simples de implementar e gerenciar, sem a necessidade de conhecimento especializado em segurança, e é suficientemente eficaz para impulsionar o Instant Recovery e crescer com sua empresa.

Conclusão

A Diretiva NIS2 foi aprovada em 17 de outubro de 2024 e adotada pela legislação dos estados-membros. Tal como no caso de qualquer decreto importante, ela exigirá esforços significativos de muitos indivíduos em organizações "importantes" e "essenciais" para garantir que não sejam multadas por não conformidade. A formação será sempre um primeiro passo fundamental para cumprir as exigências de uma legislação desse tipo. Se a Diretiva NIS2 o afetar, leia a diretiva na íntegra e garanta que sua organização esteja ciente de suas implicações. Embora no início essa iniciativa possa causar inconvenientes, a diminuição da atividade criminosa prejudicial compensará o esforço.

1.0_20251118

OBJECT FIRST