POR BRUNO CASTRO,
Fundador & CEO da VisionWare.
Especialista em Cibersegurança e Análise Forense

O QUE DIZEM OS OLHOS DA NIS2: CONFORMIDADE EM ALTA DEFINIÇÃO

A NIS2 já não é só teoria, nem apenas tema de powerpoint de conferência. Está em vigor, foi transposta, tem obrigações e multas.

A NIS2 É MUITO MAIS que uma checklist, é um teste de maturidade e se está cansado de ler informação pouco direta sobre o que isto implica, este artigo é para si.

Comecemos pelo ponto mais desconfortável: a NIS2 tira a cibersegurança da cave e leva-a para a sala do top management, já que a responsabilidade é da gestão de topo e não do "rapaz do IT", nem do fornecedor externo, nem do consultor. É de quem decide.

A adaptação começa, portanto, por governação: definir quem manda, quem decide, quem reporta e quem assume o risco. Criar (ou formalizar) um modelo de gestão de risco cibernético alinhado com o risco empresarial e integrar a segurança no mapa estratégico da organização. Se o risco digital não está lado a lado com o risco financeiro ou reputacional, então a casa ainda não está arrumada.

- Bruno Castro -
Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense

Depois vem o exercício que separa as organizações maduras de organizações otimistas: a análise de lacunas, isto é, o famoso gap analysis. E aqui é preciso honestidade brutal. Existem políticas formais? São aplicadas ou apenas assinadas? Há inventário atualizado de ativos? Sabemos exatamente que sistemas suportam processos críticos? Conseguimos identificar dependências externas? Temos registos de testes a backups ou apenas assumimos que funcionam?

A NIS2 obriga a olhar para dentro, mas também para fora, com um novo foco na cadeia de fornecimento. Fornecedores de software, prestadores de serviços cloud, empresas de manutenção remota, serviços de marketing externos, etc, todos fazem parte do perímetro real. Adaptar-se implica rever contratos, exigir garantias, introduzir cláusulas de segurança e, em muitos casos, auditar terceiros. A pergunta passa a ser: "se o meu fornecedor "cair", eu "caio" com ele?"

Em termos técnicos, não há magia, há disciplina. Autenticação multifator generalizada, segmentação de rede, gestão contínua de vulnerabilidades, patching atempado, encriptação adequada, backups offline testados, entre outros. No fundo, o que muda não é o nome das medidas, mas sim a profundidade da sua implementação.

A capacidade de deteção e resposta é outro divisor de águas. Não basta prevenir, é preciso assumir que, mais cedo ou mais tarde, algo vai falhar. Ter monitorização contínua e capacidade de resposta a incidentes (por exemplo, através de um SOC), definir procedimentos claros de escalonamento, nomear responsáveis de crise, preparar comunicações internas e externas, e acima de tudo, treinar. A diferença entre o caos e o controlo raramente está na tecnologia – está na preparação.

Há também um elemento cultural que não pode ser ignorado. A maior parte dos incidentes graves começa com um erro humano, seja um clique, uma password fraca, uma partilha indevida. Adaptar-se à NIS2 implica investir em formação real, e preparar os colaboradores para que percebam que segurança não é um obstáculo; é sim, um mecanismo de proteção coletiva.

E depois há a parte menos glamorosa: a documentação. A NIS2 exige evidências, políticas aprovadas, atas de reuniões, relatórios de auditoria, registos de formação, provas de testes. Em caso de incidente, a pergunta não será apenas "o que aconteceu?", mas também "o que fizeram para evitar?". Conseguir demonstrar diligência pode ser a diferença entre um incidente grave e um desastre jurídico.

A NIS2 é um desafio, mas pode ser igualmente uma oportunidade rara de limpar a casa a fundo, eliminar sistemas obsoletos, consolidar plataformas e repensar processos. Pode ser o pretexto certo para modernizar, para justificar investimento, para reforçar a confiança e a credibilidade junto de clientes e parceiros. Num mercado cada vez mais sensível à resiliência digital, demonstrar maturidade em cibersegurança é um argumento comercial poderoso. ■