Especialista sublinha importância de investimento em segurança das infraestruturas digitais e combater o cibercrime

expressodasilhas.cv/vOD-

O investimento em segurança da informação é essencial para garantir a seguridade das infraestruturas digitais e combater o cibercrime.A afirmação é do Ceo da Vision Ware, empresa especializada em segurança de informação, Bruno Castro, que destaca a relevância da gestão proativa e preventiva na proteção de redes, programas, sistemas, sites, aplicativos e dados contra-ataques virtuais.

“Primeiro a segurança preventiva, depois reactiva e no fim do dia a sua resiliência a ciberataques. Isto na Europa é algo que está instituído, portanto há inclusive regulações que estipulam os critérios mínimos que deve haver a este nível das infraestruturas críticas, em Cabo Verde o caminho será o mesmo a aplicar porque não haverá grandes diferenças. Nomeadamente, aqui onde temos um governo que aposta fortemente na transformação digital e na governança digital, portanto terá que ter um investimento proporcional em termos de medidas de segurança para estes mesmos serviços”, sublinha.

O especialista em investigação forense e cibersegurança chama atenção para a pertinência da análise de vulnerabilidade na antecipação, redução e correção de possíveis falhas que comprometam a ciber segurança das infraestruturas.

“Temos que estar constantemente a avaliar o nosso nível de risco. Como é que fazemos isto? É estarmos constantemente a estressar os mecanismos de segurança que protegem os ditos serviços digitais ou até as infraestruturas críticas, havendo acções de auditoria constante de forma a sermos mais robustos e mais resilientes. Não há nenhuma receita mágica, há um processo continuado que não para. É estarmos regularmente a testar, a auditar, a detectar as falhas e a corrigi-las”, explica

Para garantir e atingir os níveis necessários de segurança são necessárias boas práticas que quando aplicadas conseguem assegurar a resiliência, robustez dos sistemas.

Questionado sobre as melhores práticas para a segurança da rede em ambientes públicos, Bruno Castro, aponta sobretudo para a capacidade de manutenção dos serviços, mesmo em caso de um “desastre”.

“O que nós tentamos evidenciar nestes processos, nomeadamente quando envolve Estado, área militar, infraestruturas críticas, é que esses ecossistemas têm que ser os mais seguros possíveis. Portanto, termos isto em dois prismas, uma que é preventiva e uma que é reactiva. E é assim que nós trabalhamos, é gerir o risco numa ótica de, neste ecossistema, X ou Y, consoante a sua criticidade para o país, aplicarmos medidas mais exigentes para sermos capazes, preventivamente, de detectar um ataque, ou, no caso de sermos vítima, sermos capazes de recuperar rapidamente e efetivamente”, destaca.

“O facto de serem ambientes de administração pública ou serviços de governança digital é que qualquer ataque bem-sucedido a uma infraestrutura dessas coloque em causa serviços ao país. E, portanto, em termos de boas práticas, nós temos que fazer o mesmo que fazemos sempre, mas mais aplicados essencialmente, na capacidade de manutenção destes serviços, mesmo em caso de um desastre”, acrescenta.

O CEO da VisionWare, empresa presente em Cabo Verde há mais de 15 anos, recorda que os ataques cibernéticos são uma preocupação global e sublinha a necessidade de as entidades públicas e privadas estarem preparadas para responderem às ameaças de cibersegurança.