warpcom

"O DESENVOLVIMENTO DE COMPETÊNCIAS, CELERIDADE DE RESPOSTA E RESILIÊNCIA DAS ORGANIZAÇÕES É CRUCIAL"

Manfred Ferreira aborda o mercado de cibersegurança e os principais benefícios e riscos das organizações.

Como vê o mercado de cibersegurança?

No mercado de cibersegurança Ibérico, os clientes focam-se essencialmente no seu core business. Tal implica, num plano técnico-operacional, a passagem para a lógica de serviço e operações automatizadas em ambientes partilhados. Estamos a falar num modelo híbrido, que já desenvolvemos há cerca de cinco, sete anos, e de uma seleção natural de parceiros de confiança na criação de políticas proativas e transversais.

De que forma as organizações ficam expostas quando globalizam os seus serviços e evoluem na transformação digital do seu negócio?

A maioria das entidades em Portugal não se cinge a responder a normas e regulamentos nacionais, mas sim a normativas do mercado europeu e, em alguns casos, mundial. Este aumento de exigência, acarreta uma maior exposição a riscos de maior diversidade e complexidade. Neste contexto, o desenvolvimento de competências, celeridade de resposta e resiliência das organizações é crucial. Para tal, é aconselhável recorrer a soluções híbridas e serviços geridos que permitam ter a "visibilidade" para a tomada de decisão e a serviços complementares na cloud e data centers que garantam a "disponibilidade" necessária. Por último, deve ser garantida a cibersegurança destas soluções e serviços através de múltiplas camadas. No caso dos ambientes partilhados e distribuídos

- Manfred Ferreira -
Technical Architect
Consulting, Warpcom

como na Amazon, Azure ou Google ou através de ambientes em Cloud privada e micro redes assentes em IaaS, PaaS, DaaS e FaaS, há que garantir também a proteção dos endpoints e respetivos dados. As soluções de EPP e DLP são imprescindíveis, uma vez que asseguram a proteção contra exfiltração dos dados e documentos, aportando valor e sustendo a base da transformação digital num contexto de trabalho em qualquer localização e momento.

Como se posiciona a Warpcom face ao gap de competências existente?

A capacitação contínua dos seus especialistas é uma das fortes apostas da Warpcom. Cientes da importância dos processos de identificação de tendências e riscos de exposição das organizações, é feito um forte investimento em constantes atualizações tecnológicas juntos de parceiros de renome de cibersegurança. Do ponto de vista da oferta, detemos serviços especificamente desenvolvidos para capacitar as organizações de destreza e celeridade de reação e tomada de decisão, i.e. formação empírica com base na simulação de cenários para aplicação de técnicas de defesa e ataques cibernéticos num contexto de Cyber Range e War Game, investigação e análise forense e também a presença em grupos chave que permitem extrair previsões de antecipação de movimentos e tendências. Deste último ponto, resultam ações de mitigação dos riscos emergentes e soluções especificamente desenvolvidas para a realidade de cada organização.

Quais as principais soluções da Warpcom para o mercado de cibersegurança?

As nossas soluções de cibersegurança dividem-se, de uma forma geral, em:

- **Strategic Services** – serviços de consultoria tecnológica especializada que visam avaliar a capacidade de resposta das organizações, nomeadamente através de assessments de segurança, desenvolvimento de políticas de navegação na internet, gestão de acessos e de identidades. Também o desenvolvimento de planos de gestão de incidentes, gestão e otimização do parque e arquitetura e a revisão das soluções e de código num ciclo de CD/CI são considerados.

- **Serviços Geridos** – o Warpcom Command Center apoia na transformação e automatização de processos proativos de gestão (NOC) e proteção (SOC) das redes das empresas. Ao serem prestados por um parceiro especializado, estes serviços permitem que as organizações foquem o seu esforço e investimento no seu core business.

- **Warp Academy** – treino especializado de capacitação das equipas do cliente na resposta a incidentes, na resiliência e no apoio à continuidade do negócio. Esta tipologia de treino expõe os seus formandos a uma experiência híper-realística, baseada em cenários complexos com diferentes densidades de equipamentos, aplicações e serviços. Desta forma as equipas adquirem competências empíricas sobre como se proteger e atuar quando deparadas com ataques externos, e como conter e reverter a propagação de malwares, trojans e especificamente a proliferação de ransomware. ■