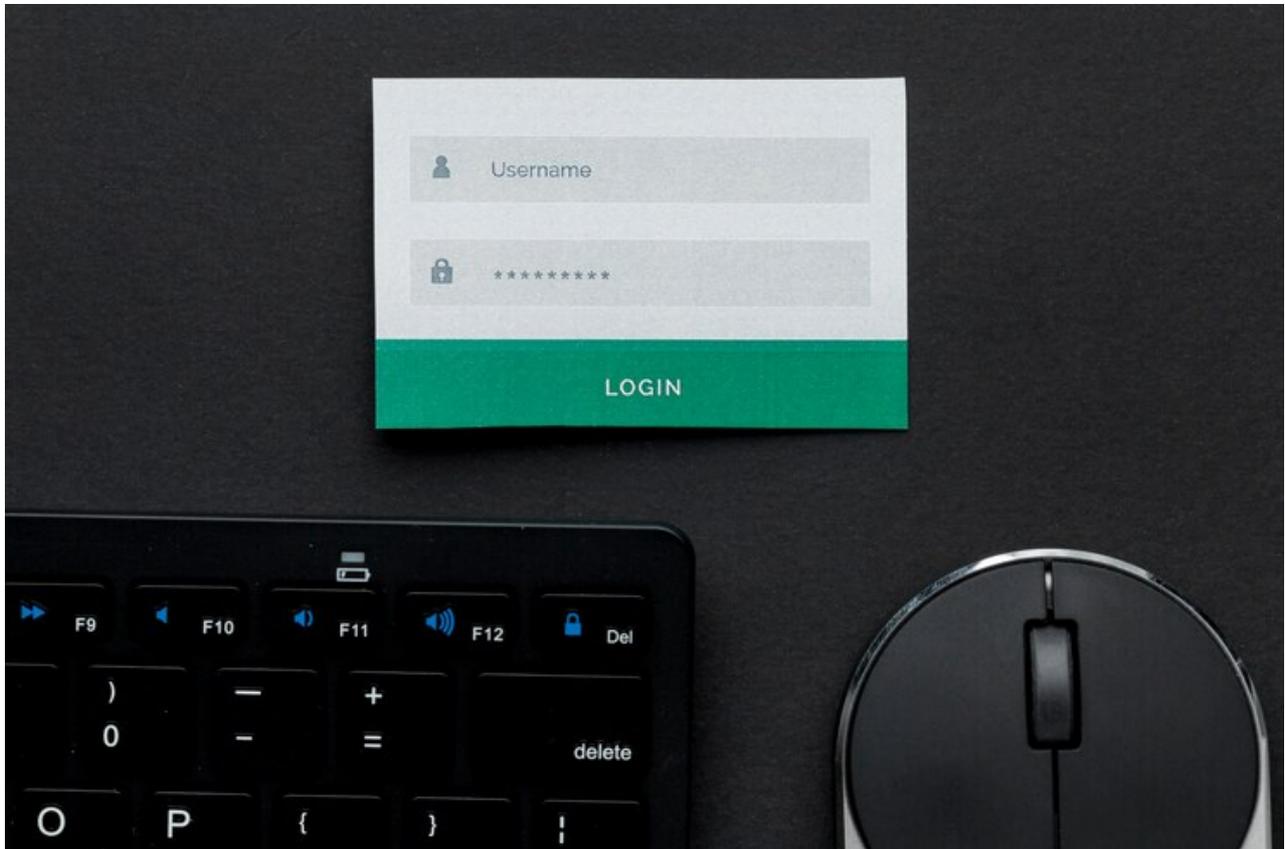


Nações Unidas abandonam Big Tech na direção de melhor privacidade e segurança [atualizado]

digitalinside.pt/nacoes-unidas-abandonam-big-tech-na-direcao-de-melhor-privacidade-e-seguranca/



O Centro Internacional de Computação das Nações Unidas (UNICC) deu um passo significativo em direção à privacidade e segurança ao selecionar a plataforma de mensagens encriptadas Element, sediada no Reino Unido, para proteger todas as suas comunicações. Este movimento reflete uma tendência crescente entre organizações que lidam com dados sensíveis, na procura de soluções que garantam maior privacidade e segurança.

A UNICC, que tem a responsabilidade do fornecimento de sistemas de tecnologia de informação e comunicação para todas as entidades das Nações Unidas há mais de 50 anos, optou pela **Element** tendo em conta a robustez em termos de criptografia da solução e soberania digital.

A escolha da **Element** por parte da UNICC significa que ter ao dispor das Nações Unidas uma plataforma que pode auto hospedar, gerir e configurar de acordo com as suas necessidades, reduzindo assim a dependência das Big Tech. Esta transição representa um marco importante na proteção das comunicações das Nações Unidas e suas afiliadas, garantindo maior autonomia e segurança na gestão de dados sensíveis.

Desde 22 de abril de 2024, todas as organizações associadas às Nações Unidas substituíram os seus sistemas de email e de chat pela aplicação **Element**, garantindo assim uma infraestrutura de comunicação mais segura e confiável. A UNICC implementou ainda funcionalidades ideais para uso empresarial, como controle avançado de identidade e acesso e auditoria, através da subscrição da **Element Enterprise**.

Este movimento segue uma tendência global de organizações, tanto públicas quanto privadas, na procura de soluções de comunicação mais seguras e soberanas digitalmente.

A transição para a **Element** representa um passo importante na proteção das comunicações das Nações Unidas e **reflete um crescente reconhecimento da importância da privacidade e segurança no ambiente digital**. Este movimento deveria inspirar outras organizações a seguir o mesmo caminho na perspectiva de procurar ter maior controle sobre os seus dados e comunicações.

Uma mudança em linha com a necessidade de fortalecer e assegurar a privacidade

Para Bruno Castro, Fundador & CEO da VisionWare, e especialista em Cibersegurança e Análise Forense, “esta decisão da ONU de adotar a Element para as suas comunicações marca um passo significativo no sentido de melhorar a privacidade e a segurança dentro da organização. Com esta decisão, a ONU está a reafirmar o seu compromisso em salvaguardar informações sensíveis e garantir a confidencialidade nas suas comunicações. A plataforma de mensagens encriptadas da Element – à partida – oferece uma solução robusta que abrange vários canais de comunicação, incluindo mensagens escritas, chamadas de voz e videoconferência, fornecendo à ONU um conjunto de ferramentas abrangente para proteger os seus dados.

Sendo a UNICC o principal provedor de serviços para o sistema da ONU que fornece serviços e soluções baseadas nas melhores práticas da indústria, padrões internacionais, seria incongruente e até irresponsável que a segurança da informação não fosse tida como uma prioridade. O ambiente de trabalho único da UNICC exige não só a melhor expertise humana, mas também que a tecnologia que sustenta todas as operações esteja em harmonia com os objetivos, ética, regulamentos e ambientes de negócios e tecnologia da ONU. Deste modo, e pelas questões sensíveis subjacentes conseguimos facilmente perceber os benefícios desta descentralização e, acima de tudo, o que isto implica em termos de soberania digital relativamente ao controlo e propriedade real dos dados que, desta forma, é detido pelo consumidor final agora com maior controlo e capacidade de personalização consoante as suas exigências e/ou requisitos – ou pelo, menos assim se espera.

Esta mudança está em linha com a necessidade de fortalecer e assegurar a privacidade e a segurança das redes internas, refletindo a dedicação da ONU em manter-se na vanguarda dos avanços tecnológicos, e em simultâneo, dá prioridade à proteção das

informações das suas partes interessadas.

As organizações que operam em diferentes países enfrentam um dilema único com a soberania dos dados: se as leis de localização de dados exigirem que os seus dados sejam armazenados dentro das fronteiras regionais, a capacidade de partilhar dados sem problemas como uma única organização fica gravemente prejudicada. Isto aplica-se tanto a entidades privadas como públicas – por exemplo, a soberania dos dados pode obstruir a partilha internacional de dados para colaborações de investigação ou esforços conjuntos de cibersegurança. Na maioria dos casos, e sendo a maioria das Big Tech americanas, o terreno onde estes data center estão localizados, bem como os dados armazenados nestes centros, são considerados ativos dos EUA.

Além da questão da soberania dos dados é ainda essencial a questão da privacidade, e como bem sabemos, as Big Tech desenvolvem produtos que muitas vezes recolhem, de forma sigilosa, informações sensíveis, as quais implicam até uma certa vigilância governamental. Por vezes, pode parecer-nos um paradoxo equilibrar a necessidade de recorrer a tecnologia de vanguarda com a necessidade de proteger dados confidenciais – felizmente, este é um exemplo de que existe essa possibilidade.”

Por sua vez João Frederico Taborda, Head of Legal da Indra Portugal, comentou ao Digital Inside que, *“a escolha do Sistema descentralizado da Element, em que a informação é encriptada mas, sobretudo, não fica armazenada em servidores das Big Tech, é um passo na autonomização dos sistemas digitais de comunicação face a quaisquer interesses nacionais. Faz sentido que a ONU, particularmente na actual conjuntura, se procure manter acima de suspeitas que podem intoxicar relações diplomáticas ou prejudicar o funcionamento das suas várias instituições. Vários países têm proposto legislação que visa regular os sistemas de comunicação digitais, nomeadamente para combate à circulação de pornografia infantil e a fraudes online, como sucedeu com o Reino Unido que aprovou em 2023 o Online Safety Act. Em teoria, porque na prática ainda não haverá meios para acesso aos servidores, este tipo de legislação põe em causa a encriptação de mensagens e a segurança da informação. Precisamente, a Element tem manifestado oposição a essa tendência regulatória, defendendo que o seu protocolo Matrix impedirá o acesso de todas as autoridades nacionais, incluindo agências de espionagem, uma vez que se baseia em encriptação end-to-end e na ausência de servidores próprios.”*