COMMUNIQUÉ DE PRESSE

Le Forum InCyber Europe 2025 planchera sur le thème : « *Zero Trust,* la confiance pour tous ? »

Il n'y a pas de confiance sans cybersécurité ; la cybersécurité repose parfois sur l'absence d'une confiance accordée a priori. Dans un monde de plus en plus hyperconnecté, transactionnel, « distribué », qui exige une cybersécurité collective et collaborative, le « *Zero Trust* » apparaît aujourd'hui comme une réponse aux enjeux démultipliés de cybersécurité.

La confiance et la sécurité ont toujours entretenu une relation ambivalente. Sans qu'il y ait de définition précise du concept de confiance numérique, il est en effet communément admis que la cybersécurité est l'une des conditions clés de la confiance. Bien que nécessaire, celle-ci ne suffit cependant pas à assurer la confiance, qu'il s'agisse de la confiance des individus « dans » les technologies numériques ou de la relation de confiance que deux individus, ou deux machines peuvent nouer via les technologies numériques. La fiabilité, la protection de la vie privée, la transparence algorithmique, l'accessibilité, l'interopérabilité sont autant d'autres critères essentiels à la confiance. Les deux notions ne se recoupent donc pas totalement. Elles diffèrent même assez largement dans leurs caractéristiques : alors que la sécurité se construit avec des mesures, des procédures, des politiques, qu'elle s'évalue avec des critères objectifs, la confiance est d'abord une croyance ou une espérance en l'identité, la fiabilité, l'intégrité ou la capacité d'un individu ou d'un système. La confiance -ou plutôt son excès- peut enfin s'opposer à la sécurité lorsqu'elle est accordée a priori et de façon implicite, c'est-à-dire sans preuves et vérification régulière de celle-ci.

Tel est justement l'apport du modèle *« Zero Trust »* : dans un monde transactionnel, où les échanges se déroulent en large partie en ligne, rendre la confiance objective en s'appuyant sur des preuves tangibles permettant de garantir que tel individu, organisation, système ou réseau, est ce qu'il prétend être et est digne de la confiance qu'il prétend mériter. Pour accéder à des ressources, applications ou données, les individus ou systèmes doivent ainsi s'identifier et être authentifiés.

FORUM INCYBER
contact@forum-incyber.com
europe.forum-incyber com

COMMUNIQUÉ DE PRESSE

C'est la fin des forteresses. Le télétravail, les organisations étendues, l'hyperconnectivité, le cloud public, l'IoT, l'extension sans fin de notre surface d'attaque et leur corollaire, la multiplication des menaces informatiques, ont eu raison de la confiance implicite qui y régnait. Voici maintenant venue l'ère du *« Never trust, always control ».*

Les technologies de gestion des identités, de contrôle d'accès, de détection et de réaction, de micro-segmentation etc. promettent ainsi une sécurité multicouches et granulaire, centrée sur les extrémités du réseau. Les technologies d'invisibilité et de leurrage progressent également. La confiance n'est donc plus accordée de façon implicite. Elle est explicite et contrôlée en permanence. Le *« Zero Trust »*, voire la méfiance, sont devenues le préalable nécessaire pour (r)établir la confiance. Un changement de paradigme qui n'est cependant pas un long fleuve tranquille : certains critiquent le « buzz marketing » autour de ce concept, quand d'autres pointent du doigt l'illusion de sécurité que ces approches procurerait, la complexité technique induite, le manque d'interopérabilité des solutions, la difficulté de l'expérience utilisateur ou bien encore leur acceptation sociétale limitée.

« Il y a un paradoxe *« Zero Trust »* car il s'agit bien de créer de la confiance par la méfiance préalable. Mais c'est sans doute le prix à payer pour un monde numérique plus sûr, souligne le Général (2S) Marc Watin-Augouard, fondateur du Forum InCyber. Ce qui est valable dans l'espace numérique se vérifie d'ailleurs aussi dans le monde réel : dans un monde incertain, les relations entre les individus, les organisations ou les Etats s'établissent de plus en plus sur la base d'une confiance explicite, s'appuyant sur des critères de conformité, des vérifications, des due diligences etc. »

« Le modèle *« Zero Trust »* comporte sans doute une part d'utopie. Mais cette utopie est vertueuse, dès lors qu'on la confronte aux réalités du terrain. L'erreur serait de penser que cette transformation n'est que technique », explique Guillaume Tissier, directeur général du Forum InCyber Europe.

FORUM INCYBER
contact@forum-incyber.com
europe.forum-incyber com

COMMUNIQUÉ DE PRESSE

La 16e édition du Forum InCyber qui a eu lieu du 26 au 28 mars 2024 a rassemblé 17 500 participants (+10%). Ses prochaines éditions auront lieu à Montréal les 29 et 30 octobre 2024, à Lille (du 1er au 1 avril 2025), à San Antonio (Texas) les 17 et 18 juin 2025.

À PROPOS DU FORUM INCYBER

Le Forum InCyber est aujourd'hui le principal événement européen sur la sécurité et la confiance numérique. L'événement, qui associe un forum, un salon et un sommet en présence de nombreuses institutions et entreprises françaises et étrangères, regroupe l'ensemble de l'écosystème de la sécurité numérique et du numérique de confiance : clients finaux, offreurs de services et de solutions, administrations, collectivités, organismes de recherches, associations.

Contacts presse :

Agence Cymbioz

fic_presse@cymbioz.com