Protection des données : pourquoi le Zero Trust a besoin de l'open source

Par Jehan Monnier, co-fondateur de Belledonne Communications

Puisque la menace est désormais à l'intérieur même de nos réseaux et face au risque d'interceptions massives en vue de l'ère quantique, le modèle Zero Trust s'impose. Mais pour être véritablement efficace, il ne doit plus s'arrêter aux portes du réseau ou des serveurs. Pour Jehan Monnier, l'application stricte du chiffrement de bout en bout, adossée à l'open source, constitue aujourd'hui l'un des meilleurs moyens de se prémunir contre les menaces et de sécuriser les communications.

La menace est déjà à l'intérieur : le fondement du Zero Trust

Le modèle Zero Trust repose sur l'idée que la menace est déjà à l'intérieur du réseau et que l'application est potentiellement compromise par défaut. La règle d'or consiste donc à ne jamais accorder de confiance par défaut et à toujours vérifier. Ce principe s'avère indispensable pour contrer la stratégie du *« harvest now, decrypt later »* (intercepter aujourd'hui, déchiffrer plus tard). Actuellement, des acteurs étatiques ou malveillants stockent massivement des communications chiffrées dans l'objectif de les exploiter lorsque la puissance de l'ordinateur quantique sera disponible. Sans défenses adaptées, d'ici une dizaine d'années, une grande partie des échanges actuels pourrait devenir publique. L'approche Zero Trust contribue à réduire considérablement les risques de collecte exploitable et de compromission des données.

Les limites du cloud et la nécessité du chiffrement de bout en bout

L’enjeu fondamental pour les organisations est de garantir des communications totalement sécurisées. Pour y parvenir, le simple recours à un hébergement souverain ne suffit plus. Il est possible d’utiliser un cloud hautement certifié (comme SecNumCloud), mais dès lors que la donnée transite ou est déchiffrée sur les serveurs, la garantie de confidentialité disparaît, notamment face aux législations extraterritoriales. Pour assurer une véritable sécurité, seul le chiffrement de bout en bout apporte aujourd’hui de réelles garanties. De nombreux services reposent encore sur le protocole HTTPS, dans lequel les données sont déchiffrées côté serveur avant d’être traitées. Pour s’affranchir de cette vulnérabilité, il est désormais nécessaire d’utiliser des systèmes à clés publiques et privées pour sécuriser les échanges indépendamment des serveurs utilisés.

L’identité et la cryptographie face aux nouvelles menaces

Sécuriser les échanges directement entre les utilisateurs crée cependant un nouveau défi opérationnel pour détecter les attaques de type « homme du milieu » (man-in-the-middle) . Le serveur ne jouant plus le rôle de tiers de confiance, il faut pouvoir vérifier de façon certaine l’identité de son interlocuteur. Pour s’assurer de cette identité, une méthode courante consistait à valider de vive voix un code de sécurité ou à scanner un QR code. Or, avec les progrès fulgurants de l’intelligence artificielle, notamment en termes de synthèse vocale, ces vérifications traditionnelles se fragilisent, rendant nécessaire une refonte des protocoles d’échange de clés.

Parallèlement, pour protéger ces échanges face aux futures capacités de calcul, l’écosystème de la cybersécurité s’oriente massivement vers la cryptographie post-quantique. Cependant, ces technologies demeurent relativement récentes et manquent encore de retour d’expérience à grande échelle. Ses potentielles failles restent à découvrir, contrairement aux standards cryptographiques historiques dont la robustesse est

éprouvée. De plus, une solution capable de résister à des attaques menées à l'aide d'un ordinateur quantique mais vulnérable aux attaques d'une machine d'ancienne génération perdrait toute son utilité. La réponse technique réside par conséquent dans le chiffrement hybride : un double verrouillage associant des algorithmes post-quantiques à un chiffrement traditionnel.

L'open source : transparence et défi du financement

Pour implémenter cette cryptographie de pointe en toute confiance, la nature du code source joue un rôle déterminant. Pour les solutions exigeant un très haut niveau de sécurité, le recours à l'open source constitue un atout majeur. Au-delà de la licence choisie, le véritable gage de confiance réside dans la capacité technique de l'utilisateur à inspecter et recompiler lui-même son application. Néanmoins, le choix de modèles open source très stricts pour le code freine souvent la monétisation classique, ce qui soulève le défi structurel du financement. Sans revenus prévisibles, comment assurer la mobilisation continue d'ingénieurs qualifiés pour maintenir ces briques cryptographiques complexes ? Le modèle de la double licence apporte une réponse concrète. En commercialisant des licences propriétaires du code open source auprès des entreprises qui refusent de partager le leur, c'est finalement l'écosystème logiciel propriétaire qui finance l'innovation ouverte et sa pérennité.

Écoutes numériques et chaîne de responsabilités globales

Si la transparence du code est essentielle, elle s'inscrit dans un contexte géopolitique où la lucidité est de mise. L'interception des communications est une pratique historique et généralisée à l'échelle mondiale. Aucune réglementation ne met les organisations totalement à l'abri des écoutes. La véritable différence réside dans l'encadrement juridique : si l'Europe impose l'autorisation stricte d'un juge, un citoyen étranger soumis aux dispositifs de surveillance prévus par

certaines législations nord-américaines ne bénéficie d'aucune garantie, s'exposant à une collecte massive.

En définitive, la confiance numérique exige de bâtir une chaîne de responsabilités technologiques de bout en bout. Le logiciel de communication doit impérativement garantir un chiffrement robuste . Mais cette sécurité logicielle doit s'inscrire dans une réflexion plus vaste incluant le matériel. Même en utilisant des composants importés dont la sécurité absolue ne peut être prouvée, il demeure possible de limiter les risques en contrôlant strictement le système d'exploitation qui les anime.

Tourner le dos au modèle Zero Trust aujourd'hui, c'est renoncer à la sécurité de demain. S'appuyer sur la transparence de l'open source, associée à une cryptographie hybride robuste, reste à ce jour la méthode la plus crédible pour reprendre la maîtrise de ses données.

À propos de l'auteur : Jehan Monnier est cofondateur de Belledonne Communications, éditeur à l'origine de la solution open source Linphone. Ingénieur de formation, il promeut depuis plus de quinze ans une approche souveraine et interopérable des communications IP en s'appuyant sur des standards ouverts. Il accompagne aujourd'hui les entreprises et les collectivités dans leurs projets de téléphonie en proposant des alternatives aux solutions propriétaires.