PATRICK BARBEY
Directeur d'Innovaud

ENTRETIEN

Innovaud, partenaire de la conférence « Cyberrisques » répond à nos questions sur les innovations en terme de cyberespace.

Le canton de Vaud est reconnu pour son grand nombre d'entreprises spécialistes en cybersécurité. De quelle manière assurez-vous leur promotion ?

En effet, nous avons la chance de compter deux institutions significatives en la matière: l'EPFL et l'HEIG-VD. Plusieurs startups sont sorties de ces deux écoles et d'autres sont en collaboration avec des labos et instituts sur des thématiques de pointe. Parmi les secteurs qui sont prioritaires pour nous (Sciences de la Vie, ICT, Industrie de Précision et efficacité énergétique), nous avons défini 14 domaines d'innovation où le Canton a une position compétitive au niveau mondial; le domaine de la Cybersécurité fait partie de cette liste.

Le soutien aux entreprises de ce secteur se fait sur quatre axes principaux. Le financement, où nous pouvons soutenir les innovateurs avec des montants pouvant atteindre 500'000.-. Le coaching, avec un réseau de 80 spécialistes de différents secteurs. L'hébergement avec les 6 technopôles que compte le canton.
Et finalement la promotion à proprement parler, avec des portraits d'entrepreneurs réalisés par des journalistes, vidéos professionnelles afin de mieux les faire connaître. Notre présence sur les réseaux sociaux permet de diffuser cette information. La promotion recouvre aussi les événements que nous organisons et où nous mettons en avant les startups et entreprises innovantes.

Quelles évolutions avez-vous pu observer quant à l'innovation par rapport aux moyens de protection contre les cyberrisques ?

Parmi les innovation en la matière on peut relever l'utilisation de l'intelligence artificielle et plus particulièrement du «deep learning», qui peut mettre en évidence des attaques sur la base d'indices très diffus, qui échappent aux experts.

Un autre domaine en plein développement est la protection avant attaque, qui permet de se protéger préventivement des virus et autres malwares. Aujourd'hui la plupart des anti-virus essayent de détecter l'infection une fois qu'elle a eu lieu ou pendant qu'elle s'exécute.

On peut également citer le «app hardening», dont l'objet est de rendre une application très difficile à comprendre et donc à limiter le risque de rétro-ingénierie par des entreprises concurrentes ou par des hackers.