La bourse de Zurich: photo du 21 juillet 1960. Elle fait partie d'un reportage de 141 photos. *(ETH-BIBLIOTHEK ZÜRICH, BILDARCHIV/FOTOGRAF: METZGER, JACK)*

Ce logiciel anti-fraude né à Cyber-les-Bains

CRIMINALITÉ Les programmes auto-apprenants de NetGuardians contrôlent les irrégularités dans les transactions en temps réel. L'entreprise est au cœur du cluster informatique d'Yverdon-les-Bains

FREDY HÄMMERLI

En 2016, des criminels restés inconnus ont détourné sur leurs propres comptes un total de 951 millions de dollars appartenant à la banque centrale du Bangladesh. Grâce à une simple faute de frappe, ce ne sont finalement «que» 81 millions de dollars qui ont définitivement disparu. Cette même année, des cybercriminels ont réussi à pirater 20 000 comptes de clients de la banque britannique Tesco, et leur butin a atteint 2,5 millions de livres. En mars dernier, des criminels ont craqué le compte bancaire d'une entreprise suisse et transféré 1,2 million de francs sur un compte au Kirghizistan.

La liste peut être allongée à l'envi. Des cyberattaques se produisent quotidiennement, surtout contre des banques et autres prestataires financiers. Melani, la centrale suisse d'enregistrement et d'analyse de la cybercriminalité, a dénombré en 2017, rien que pour la Suisse, 4587 sites de phishing. A quoi s'ajoutent d'innombrables attaques de logiciels malveillants et de pirates. Plus de 870000 paquets de données ont été compromis l'an dernier. L'identification à deux facteurs, censée conférer plus de sécurité aux données délicates, est la cible d'attaques la plus récente.

Cybercluster à Yverdon

En général, les hackers opèrent depuis l'étranger mais se cachent souvent derrière de pseudo-adresses suisses, les «mule-accounts». L'Association of Certified Fraud Examiners, une organisation internationale sans but lucratif et ses 65000 membres qui se vouent à la lutte contre la criminalité économique et le crime organisé, estime à 67 milliards de dollars par an les préjudices causés de par le monde. Sans compter le dommage de réputation.

Souvent, la tentative de piratage se solde par un échec. Mais les hackers réussissent parfois leur coup. «Trop souvent», juge Joël Winteregg, CEO de NetGuardians, un producteur de logiciels domicilié dans la paisible cité d'Yverdon-les-Bains. NetGuardians est une start-up fondée en 2007. Depuis 2011, elle s'est spécialisée dans les logiciels détecteurs de fraudes à l'usage des banques. Elle figure ainsi parmi la dizaine d'entreprises de la planète qui se consacrent à cette spécialité et la seule et unique de Suisse.

Le fait qu'elle ait vu le jour à Yverdon-les-Bains est lié au cluster qu'abrite cette ville qui s'est vu octroyer le surnom de Cyber-les-Bains et qui est désormais presque aussi renommée que la Crypto-Valley de Zoug. L'Y-Parc et ses multiples start-up dans le secteur des fintechs, la proximité de l'EPFL et de la Haute Ecole vaudoise d'ingénierie (HEIG), sans parler du groupe technologique Kudelski spécialisé dans la sécurité, compensent largement la distance avec les grands centres bancaires.

Le logiciel anti-fraude de NetGuardians a une certaine avance sur les systèmes jusqu'ici utilisés dans les banques: il n'analyse pas que les transactions louches qui sautent aux yeux mais contrôle un à un, automatiquement et en temps réel, tous les mouvements. Il ne scanne pas seulement les montants visiblement importants, les devises inusitées ou douteuses, les temps de transaction, l'expéditeur et le destinataire, mais un ensemble de quelque 300 paramètres. Parmi lesquels les habitudes de paiement d'un client, le navigateur qu'il utilise et même la définition de son écran.

Toutes ces informations sont recoupées avec un modèle de risque fondé sur l'intelligence artificielle. Si un ou plusieurs des critères divergent du comportement habituel du client, le système sonne l'alerte et bloque la transaction. Les nouveaux clients, dont les données ne sont pas encore suffisamment connues, sont recoupés avec le modèle de comportement de groupes de pairs analogues.

Le logiciel analyse tout aussi finement le comportement des collaborateurs. Car la statistique révèle que 70% de toutes les tentatives de fraude sont réalisées avec l'aide d'initiés, le plus souvent des collaborateurs. Des tests exhaustifs sur une année dans une banque avec son système de règles usuel et avec la solution de NetGuardians ont montré un résultat amélioré de 18% pour l'entreprise yverdonnoise. Et les pertes ont été réduites de 60%, sans parler d'un gain de temps de 93%. «Notre logiciel a déjà permis à plusieurs clients bancaires d'être préservés de pertes», assure Joël Winteregg, CEO de NetGuardians.

Les fausses alertes sont rares

Selon un inventaire de NetGuardians, le logiciel auto-apprenant est tellement malin que le nombre des redoutés «false positives», comme on appelle les fausses alertes chez les spécialistes, est de 83% plus bas qu'avec les méthodes traditionnelles. Cela dit, le logiciel de NetGuardians n'est pas la panacée contre le blanchiment d'argent, la corruption, la violation des règlements ou le financement du terrorisme. Contre ces crimes, la banque doit se battre en recourant à des logiciels complémentaires et surtout à l'aide d'une culture d'entreprise axée sur la bonne gouvernance.

Une cinquantaine de banques de 15 pays sont désormais équipées du logiciel anti-fraude de NetGuardians, la moitié d'entre elles en Suisse, l'autre moitié au Luxembourg, en Grande-Bretagne, mais surtout en Afrique, au Moyen-Orient et en Asie du Sud-Est. De sorte que NetGuardians entretient des postes avancés à Nairobi et à Singapour. Mais la Suisse alémanique et ses grandes banques, l'Europe et l'Amérique sont également dans le collimateur de NetGuardians.

Croissance à toute allure

NetGuardians emploie aujourd'hui 80 personnes, dont la moitié à son nouveau siège d'Yverdon-les-Bains. Quinze programmeurs travaillent à Varsovie. Il y a un an encore, l'entreprise comptait 56 collaborateurs seulement. Le chiffre d'affaires devrait atteindre 6 millions de francs cette année et l'on s'attend à ce que cela continue au même rythme. «Nous entendons doubler le chiffre d'affaires chaque année», annonce Joël Winteregg. Le modèle d'affaires doit évoluer rapidement et continuer de s'ancrer à l'étranger. Les partenariats avec Swisscom, Avaloq, Adnovum et Temenos y contribueront, et d'autres partenariats sont prévus.

Pour pouvoir tenir la cadence, Joël Winteregg et son cofondateur, Raffael Maio, ont besoin d'argent frais. Jusqu'ici, ils ont trouvé 14,5 millions de francs chez Swisscom et chez des entreprises de capital-risque, comme Polytech Ventures. Ils détiennent encore tout juste la moitié des actions de NetGuardians. L'année prochaine, 30 millions supplémentaires devraient arriver. «Mais à moyen terme, nous visons une mise en bourse ou la fusion avec un groupe international.» ▬

«POUR LA PREMIÈRE FOIS, GRÂCE À L'ANALYSE DES CLIENTS, LES FRAUDEURS N'ARRIVENT PAS À SUIVRE»

INTERVIEW

NOM: JOËL WINTEREGG
FONCTION: CEO NETGUARDIANS

Joël Winteregg dirige NetGuardians avec son cofondateur, Raffael Maio. Il détient un diplôme d'ingénieur logiciel et de Certified Information Systems Security Professional. Il s'occupe surtout du développement technologique et des activités de NetGuardians en Europe et en Afrique.

Comme mentionné ci-dessus, la banque centrale du Bangladesh et Tesco Bank comptent parmi les innombrables victimes de fraudes. Votre logiciel anti-fraude aurait-il pu empêcher ces cas-là ou des cas similaires? Absolument. Nous avons même réalisé des simulations de ces cas. Il s'agit certes de formes de fraude extrêmement sophistiquées, mais elles ont toutes laissé des traces que nous avons découvertes à temps et aurions ainsi pu empêcher. Dans le cas du Bangladesh, notre logiciel aurait pu immédiatement sonner l'alerte en raison des montants élevés, du moment inhabituel (pendant le week-end) et du destinataire inhabituel (un casino des Philippines).

Comment la Suisse se situe-t-elle en comparaison internationale? Hélas, pas mieux qu'ailleurs. Les banques ont beaucoup d'expérience de la défense contre les fraudes fondée sur des règles. Par exemple, les versements dans des pays critiques éveillent tout de suite l'attention. Mais ça ne suffit plus. Les gens utilisent leur carte de crédit pendant un bref séjour en Thaïlande et en profitent pour acheter en ligne en Chine. Notre logiciel analyse le comportement des clients et constate que de telles transactions peuvent être parfaitement normales parce que le client concerné a réservé auparavant un voyage en Thaïlande et qu'il s'approvisionne régulièrement chez Alibaba. La Grande-Bretagne et l'Irlande, avant tout, ont de l'avance sur nous parce qu'elles sont confrontées depuis bien des années aux tentatives de fraude.

Où en est-on aujourd'hui de l'incessante compétition entre gendarmes et voleurs? Si nous n'utilisons qu'une défense fondée sur des règles, les fraudeurs auront une étape d'avance sur nous. Grâce à l'analyse des clients et au recours à l'intelligence artificielle, on a la situation inverse: pour la première fois, les fraudeurs n'arrivent pas à suivre. ▬

Interview: Fredy Hämmerli