Telle était la 26e édition des

DATA NEW

Bart Preneel, cryptographe de renommée mondiale, analyste crypto et professeur à la Katholieke Universiteit Leuven, a été élu ICT Personality of the Year 2025 dans le cadre des Data News Awards for Excellence, un événement qui a également couronné 13 entreprises.

Les Data News Awards for Excellence organisés le 15 mai dernier ont surpris le secteur belge de l'ICT, non seulement par la traditionnelle reconnaissance des leaders technologiques nationaux, mais aussi par un déménagement exceptionnel. En effet, après 25 éditions organisées dans la métropole bruxelloise, le tapis rouge a été déroulé cette fois dans le Studio 100 Pop-Up Theater de Puurs. Sous la direction de la présentatrice Ruth Beeckmans et avec une touche de glamour de Las Vegas, le show restera certainement dans la mémoire de tous les invités. Ne serait-ce que parce qu'il s'agit là du dernier événement B2B de prestige avant la démolition définitive du Pop-Up Theater.

Bart Preneel se positionne non seulement comme un visionnaire, mais aussi comme une boussole morale.

Treize entreprises ont reçu un award tant convoité pour leurs performances dans différents domaines de l'ICT, preuve que l'innovation et la vision stratégique ne sont nullement une question de chance. L'apothéose était incontestablement l'annonce de l'ICT Personality of the Year. Le professeur Bart Preneel (KU Leuven), une autorité en matière de cryptographie et de cybersécurité, s'est vu décerner ce prix prestigieux. Il l'a emporté face à 4 autres nommés – Leen Anthuenis (Supernova & Startups.be/Scale-Ups.eu), Steven Latré (Openchip & Universiteit Antwerpen), Phedra Clouner (Centre for Cybersecurity Belgium) et Michel Verwaerde (GTT) – dont les noms ont été dévoilés au cours de la soirée même par le biais de dés géants gonflables lancés dans le public. Mais le jackpot a finalement été remporté par Preneel dont la contribution au secteur a été unanimement reconnue.

La réception d'accueil et la remise des prix ont été suivies d'un dîner de gala et d'une soirée de réseautage. Cette soirée était placée sous le signe du sourire, et pas seulement chez les lauréats qui se sont vu remettre un award. Pour décerner les différents prix, nous avons pu compter sur vous, cher lecteur, ainsi que sur notre jury professionnel. Comme chaque année, vous avez pu voter pour vos fournisseurs, entreprises et produits ICT favoris dans 13 catégories.

Comment se déroulait la procédure ?

Les entreprises avaient l'occasion de se présenter pour une première sélection, le tout complété par la rédaction. Vous avez ensuite voté massivement via notre site Web pour choisir vos favoris, ce qui a ramené chaque catégorie à un top 5. Par la suite, notre jury professionnel s'est basé sur ce top 5 pour désigner le vainqueur final dans chaque catégorie. La réunion du jury, les discussions et les votes ont eu lieu dans les bureaux de Data News. Durant ces 4 dernières années, une tendance s'est dégagée à choisir davantage d'entreprises belges comme lauréates, une évolution qui s'est confirmée cette année encore. Les clients optent fréquemment pour des acteurs locaux et cherchent souvent un ancrage local auprès des entreprises internationales et des multinationales. Nous vous présentons dans les pages suivantes tous les lauréats et les nommés des 13 awards.

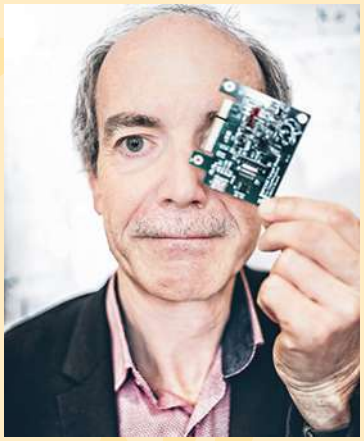
S AWARDS

Bart Preneel est l'ICT Personality of the Year

Le 14e award est celui de l'ICT Personality of the Year, un prix exclusivement sélectionné et attribué par la rédaction. Cette ICT Personality of the Year est choisi dans une liste de 50 grosses pointures du monde ICT belge. Il doit s'agit d'un Belge ou d'une personne résidant depuis un certain temps déjà en Belgique, et qui a marqué durablement le secteur ICT belge ou a eu une influence majeure sur l'écosystème ICT en dehors de nos frontières. Après délibération, la rédaction a ramené cette liste à 5 candidats potentiels pour ce prix prestigieux. Cette année, le choix de la rédaction s'est finalement porté sur Bart Preneel pour le rayonnement international de ses travaux en cryptographie et son impact moral. En tant que responsable du labo Cosic de la KU Leuven, il est connu de tous pour être celui qui a réussi à pirater les voitures Tesla, une prouesse qu'il a réalisée pour permettre de sensibiliser le monde aux questions de sécurité tout en repoussant les limites de l'innovation en matière de cybersécurité. Bart Preneel suit de très près les nouvelles législations susceptibles de mettre en péril la vie privée des citoyens et s'efforce, à l'instar de ses collègues-professeurs dans l'ensemble de l'Europe, d'impacter sur les choix politiques. Il se profile non seulement comme un visionnaire, mais aussi comme une boussole morale. Et cette boussole ne se limite aux frontières de notre pays. En fait, il est impossible de ne pas surestimer le rayonnement de Bart Preneel sur notre société, ce qui explique que la rédaction soit particulièrement fière de pouvoir distinguer un tel pionner en lui attribuant le titre d'ICT Personality of the Year de Data News. Son interview complète est à lire dans la suite de ce magazine.

Kristof Van der Stadt

ICT Personality of the Year: Hall of Fame



2025 Bart Preneel
2024 Mitch De Geest
2023 Luc Van den hove
2022 Jan Hollez
2021 Fabien Pinckaers
2020 André Knaepen
2019 Daan De Wever
2018 Françoise Chombar
2017 Felix Van de Maele
2016 Jonas Dhaenens
2015 Jürgen Ingels
2014 Dries Buytaert
2013 Eric Van Zele
2012 Sophie Vandebroeck
2011 Jan Valcke
2010 Jo Cornu
2009 Alain Wirtz
2008 Pierre De Muelenaere
2007 Gilbert Declerck
2005 Robert Cailliau

Qui siège au sein du jury ?

Le jury se compose du CIO of the Year et d'anciens lauréats, de présidents de groupements d'utilisateurs et de personnalités indépendantes du biotope ICT belge et de membres de la rédaction de Data News. L'assemblée du jury s'est tenue cette année dans les bureaux de la rédaction de Data News chez Roularta Media Group. Seuls les membres présents ont pu exprimer leur vote.

Les membres du jury invités étaient :
An Swaelens (CIO of the Year 2023), **Bart Steukers** (Agoria), **Cassandre Laurent** (Agence du Numérique), **Egide Nzabonimana** (Isaca), **Elke Laeremans** (CIO of the Year 2021), **Erik Cuypers** (MIT-Club), **Frank Robben** (Smals), **Geert Goethals** (CIONET), **Jack Hamande** (BOSA), **Sonia Vermeira** (ADM), **Kristof Van der Stadt** (Data News), **Els Bellens** (Data News), **Leen Anthuenis** (StartUps.be/Scale-Ups.eu), **Levi Nietvelt** (Beltug), **Marc Senterre** (CfTDN), **Marc Vael** (SAI), **Peter Vermeylen** (CIOforum), **Philippe Van Belle** (CIO of the Year 2022), **Stijn Viaene** (Vlerick), **Tony Mary** (TM Consulting).

Et les gagnants sont...

Data News a récompensé dans 13 catégories les meilleures entreprises dans leur domaine. Tous les nommés sont certes des leaders dans leur secteur, mais le jury a sélectionné à chaque fois son favori.

BELGIAN TECH SCALE-UP COMPANY OF THE YEAR

Lighthouse

L'année a été excellente pour Lighthouse. Cette plateforme de données pour hôtels est notamment parvenue à se distinguer par un nouveau tour de table financier, ce qui permet à l'entreprise fondée voici désormais 12 ans de rejoindre le club select des licornes belges.

Autres nommés : Loop Earplugs, Nviso, Odoo, TechWolf

BELGIAN TECH START-UP COMPANY OF THE YEAR

Aikido Security

Chaque année, le jury s'intéresse aux jeunes start-up prometteuses dans toute une série de secteurs. Cette fois, une entreprise de staffing entrait en ligne de compte, outre 3 jeunes pousses en IA. Le prix a finalement été attribué à la toute jeune Aikido Security, une société ultra-technologique qui scanne le code à la recherche des vulnérabilités.

Autres nommés : Dark Light, Lucy, Paperbox, Limecraft

CUSTOMER CENTRIC IT COMPANY OF THE YEAR

GTT

Un prix particulièrement convoité dans la mesure où des clients satisfaits représentent un atout majeur pour nombre d'entreprises. Cette année, GTT remporte cette catégorie. L'entreprise a brillé dans l'enquête Whitelane sur la satisfaction des clients et marque son retour en force après quelques années délicates.

Autres nommés : delaware, iO, Proximus, Tata Consultancy Services

BUSINESS COMMUNICATIONS
INNOVATOR OF THE YEAR

Proximus NXT

Cette catégorie regroupe chaque année pratiquement les mêmes noms. Proximus NXT l'emporte cette fois grâce à des investissements importants dans de nouvelles technologies, comme les réseaux quantiques.

Autres nommés : Citymesh, Dstny, Mobile Vikings, Orange

DATA CENTER SERVICES
COMPANY OF THE YEAR

NTT Data

Pour se distinguer, les services de centres de données se doivent d'être durables, d'innover et, en ces temps géopolitiques troublés, d'offrir différentes options internationales. NTT Data coche ces différentes cases, avec notamment un label d'or EcoVadis de durabilité et centre d'innovation à Bruxelles.

Autres nommés : Atos, Cegeka, Kyndryl, NRB

CYBERSECURITY
COMPANY OF THE YEAR

Cegeka

Cette catégorie comprenait cette année plusieurs acteurs belges majeurs. Cegeka l'a finalement emporté. Ces dernières années, cette entreprise s'est positionnée comme un spécialiste de la cybersécurité et a réalisé un beau parcours selon le jury.

Autres nommés : Cyber Security Management, Inetum, Nviso, Proximus NXT

ARTIFICIAL INTELLIGENCE
INNOVATOR OF THE YEAR

Google Cloud

L'année dernière, cette catégorie avait été remportée par le fondeur Nvidia. Mais cette année, le public a voté pour un spécialiste du logiciel qui a réussi à intégrer l'intelligence artificielle dans ses applications. Une mention spéciale a été attribuée aux services de Cronos.ai, mais le jury a finalement choisi Google Cloud, qui est parvenue ces derniers mois à améliorer sensiblement ses modèles d'IA, dont Gemini.

Autres nommés : Cronos.ai, element61, Salesforce, ServiceNow

→

ENTERPRISE APPLICATION
INNOVATOR OF THE YEAR

Odoo

Quelques acteurs disparates dans cette catégorie, mais le prix a finalement été attribué à la perle belge Odoo. Le jury a particulièrement apprécié l'évolution énorme et l'innovation continue de la scale-up qui s'est fortement renforcée ces dernières années tout en continuant à respecter ses valeurs clés, comme la focalisation sur l'open source.

Autres nommés : AE, Easi, Microsoft, Visma

ENTERPRISE IT SERVICES
COMPANY OF THE YEAR

Cronos Groep

Dans cette catégorie, Data News a établi une distinction entre les prestataires de services pour moyennes entreprises (en fonction des revenus) et pour grandes entreprises, sous le nom 'enterprises'. Du coup, il s'agissait là de la catégorie la plus disputée lors du vote. Finalement, Cronos l'a emporté, suivie de très près par Tata Consultancy Services.

Autres nommés : Accenture, Deloitte, NTT Data, Tata Consultancy Services

IT RECRUITING & SOURCING
COMPANY OF THE YEAR

Talent-IT/Harvey Nash

Le jury distingue Talent-IT en raison du fait qu'elle ne se limite pas à placer des profils, mais investit massivement dans la formation et l'accompagnement, tout en présentant des profils plus variés et inclusifs.

Autres nommés : Amon Consultants, IT-Planet, Randstad Digital Belgium, Vibe Group

CLOUD & IT INFRASTRUCTURE
INNOVATOR OF THE YEAR

Microsoft

À nouveau une catégorie où l'on rencontre quelques noms connus. Microsoft l'emporte ici grâce à son expertise en services cloud, mais aussi du fait qu'elle s'investit souvent dans la réflexion de ses clients.

Autres nommés : Amazon Web Services, Google Cloud, Kyndryl, Oracle

IT SERVICES
SMB OF THE YEAR

AE

Cette catégorie revient à AE pour son approche spécifique. En tant que prestataire de services, l'entreprise prend comme point de départ l'architecture tout en s'impliquant étroitement dans l'environnement de son client, qu'il s'agisse d'une grande ou d'une plus petite entreprise.

Autres nommés : Computerland, ConXioN, Devoteam, VanRoey

MOST SUSTAINABLE ICT
COMPANY OF THE YEAR

Cegeka

Pour cette catégorie, les entreprises doivent présenter elles-mêmes leurs arguments. Cegeka s'est montrée la plus convaincante. L'entreprise est auto-suffisante et se fixe un large éventail d'objectifs en durabilité, sur le plan tant écologique que social. Elle se montre en outre ambitieuse et entend notamment imposer à l'avenir à ses fournisseurs de respecter certains standards.

Autres nommés : Atos, delaware, Easi, NRB

Els Bellens

« Nous sommes en train de créer une sorte de super-outil pour dictateurs »

Bart Preneel figure parmi l'élite mondiale de la cryptographie et est par ailleurs une voix reconnue pour la défense de la vie privée des citoyens. Nous parcourons avec lui l'histoire de l'espionnage, des clés et du scanning.

La rédaction de Data News a élu cette année Bart Preneel comme ICT Personality of the Year. Ce professeur est depuis quelques années déjà la tête du département Sécurité informatique et Cryptographie industrielle à la KU Leuven.

Vous êtes ingénieur en électrotechnique de formation. Votre ambition a-t-elle toujours été de devenir cryptographe ?

BART PRENEEL: Pas vraiment. J'ai consacré ma thèse aux modems de Telindus, qui sera rachetée ensuite par l'actuelle Proximus. Pour mon doctorat, j'ai rencontré le professeur Joos Vandewalle qui m'a convaincu d'entamer des recherches en cryptographie. A l'époque, le COSIC [le groupe de recherche en sécurité informatique et en cryptographie industrielle, NDLR] manquait de chercheurs. Ce groupe avait été établi en 1978 et était une première en Europe avec la création d'une start-up spécialisée en puces. Bon nombre d'entre eux avaient quitté en 1986 pour fonder une spin-off. J'étais le premier volontaire à se proposer dans ce domaine et je me suis donc lancé dans la cryptographie. À l'époque, c'était pourtant nettement plus facile qu'aujourd'hui. La recherche dans ce domaine tenait dans une demi-armoire et sa consultation permettait d'en savoir autant que tout le monde, à moins de travailler pour le secteur public.

Pourquoi êtes-vous resté ?

PRENEEL: Il s'agissait d'une combinaison très intéressante entre la recherche mathématique et l'impact sociétal. Je ne pense pas que l'on se rendait compte à l'époque qu'une percée majeure allait se produire. Lorsque j'ai débuté en 1987, la cryptographie se limitait aux banques et au secteur public, voire à la diplomatie et à l'armée. Mais c'était pratiquement tout. Avec l'émergence de l'Internet, le domaine s'est fortement élargi en quelques années à peine. Et au milieu des années 90, la cryptographie a également été possible au niveau logiciel. Soudainement, une sorte de produit de masse est apparu qui allait aussi avoir des répercussions politiques.

Vos premières recherches ont porté sur les fonctions de hachage. De quoi s'agissait-il ?

PRENEEL: Au départ, l'attention s'est surtout portée sur la sécurisation de l'information sans fil contre les écoutes. Or le secteur financier était surtout inquiet de l'altération de transactions. Car lorsqu'il devient possible de transformer une transaction de 1.000 en 1 million $, l'impact financier est énorme.

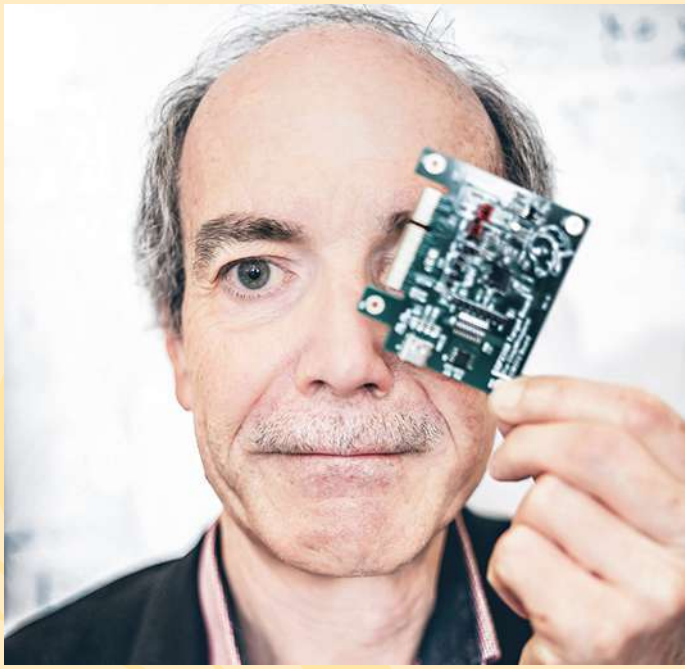
Pour détecter si un message est ou non modifié, on a eu recours à une clé numérique. C'est ce que l'on fait aujourd'hui encore avec le hachage. Lorsque vous faites un paiement, on mélange les données de la transaction à l'aide d'une clé, après quoi on ajoute quelques octets au message. Par la suite, il est possible d'utiliser la même clé pour faire la vérification. Et si le résultat ne correspond pas, c'est qu'il y a eu altération.

Vous êtes notamment à l'origine de la fonction de hachage Miyaguchi-Preneel.

PRENEEL: Il s'agit d'une méthode qui permet de générer une fonction de hachage sans clé →

LANGER
IC - Scanner FLS 102

d'un bloc de cryptage. Les fonctions de hachage ont été utilisées dans les années 80, notamment lorsque les courriers d'entreprise venaient collecter les bandes magnétiques des mainframes. Ces bandes renfermaient toutes sortes de fiches de salaire ou de transactions d'une entreprise qui devaient être transmises à la banque. Or il existait un risque que le courrier soit intercepté en chemin et que les données soient modifiées. Pour éviter ce risque, les transactions stockées sur bande ont été réduites à un fichier très petit. Le CFO communiquait ceci à la banque qui pouvait alors savoir si une modification était intervenue. L'un de mes premiers thèmes a donc été ce type de fonction de hachage.



Sont-elles encore utilisées de nos jours ?

PRENEEL: Chaque appli que vous installez aujourd'hui sur votre téléphone ou votre ordinateur portable est signée numériquement à l'aide d'une fonction de hachage. Au fil du temps, ces concepts mathématiques n'ont pas changé. Les algorithmes ont été adaptés en partie, mais le Miyaguchi-Preneel est un concept qui peut s'appliquer aux blocs de cryptage plus modernes. C'est une manière de changer une seule chose dans une autre.

Un autre algorithme auquel j'ai contribué est RIPEMD-160. Je l'ai conçu avec mon collègue Antoon Bosselaers dans le cadre d'un projet européen développé en collaboration avec Hans Dobbertin de la BSI [le pendant allemand du CCB, NDLR]. Nous voulions imaginer une alternative au fameux standard logiciel MDS. Dans les années 90, on commençait déjà à s'apercevoir que celui-ci n'était pas tellement sécurisé. Ce MIPEND-160 est une fonction de hachage plus robuste tout en étant efficace. Elle est notamment utilisée par des banques allemandes et suisses. Et elle n'a toujours pas été cassée. Et en 2008, elle a d'ailleurs été intégrée dans le bitcoin par Satoshi Nakamoto. Si vous avez une clé publique dans le bitcoin, celle-ci sera hachée avant de l'envoyer pour créer une adresse bitcoin. Et c'est là qu'intervient RIPEMD-160. Donc, quelque chose que j'ai contribué à créer en 1996 est intégré à chaque transaction bitcoin. Mais c'était impossible à prédire.

L'idée prévaut que ce type de technologie évolue très rapidement ? En va-t-il de même de la cryptographie ?

PRENEEL: Nos perceptions changent en tout cas. Il faudra par exemple toujours des clés plus puissantes. L'un des principaux standards remonte à 1977 et utilisait 56 bits. Ceci a été choisi sciemment parce que seule a NSA [les services secrets américains, NDLR] disposait de la puissance de calcul nécessaire pour craquer ce standard, à l'inverse du reste du monde. C'est d'ailleurs pourquoi l'agence a pu rendre celui-ci public et permettre à d'autres organisations de l'utiliser.

Et il en va de même pour des développements plus récents. Toutes les clés proposées jusque dans les années 2000 étaient, sous la pression des autorités, plus courtes qu'elles auraient dû être. Aujourd'hui, cette question est en partie résolue et les clés cryptographiques actuelles sont suffisamment longues. Désormais, on s'intéresse surtout aux clés qui exploitent au maximum les logiciels existants.

Mais de temps à autre, certaines clés sont craquées. Dans les années 90 par exemple, le monde entier utilisait ce standard MD5. Microsoft avait ainsi quelque 800 applications de MD5 dans Windows. Or en 2004, le professeur chinois Wang a démontré lors d'une conférence qu'il était possible de craquer cette clé en 15 minutes. Du coup, une migration de grande ampleur a été nécessaire.

Et on voit désormais apparaître l'informatique quantique.

PRENEEL: Il s'agit en effet de la grande migration qui nous attend. Bon nombre de nos algorithmes ont été imaginés dans les années 90. Ceux-ci sont utilisés dans tout, depuis les protocoles en ligne jusqu'au design de mises à jour, mais aussi pour les cartes d'identité et les passeports. D'après moi, quelque 50 milliards de transactions s'appuient sur de tels algorithmes.

Or il apparaît désormais que de tels algorithmes

n'offrent plus de sécurité s'il devient possible de construire un ordinateur quantique suffisamment grand. Ces algorithmes génèrent certes de très grands chiffres et nous n'en sommes donc pas encore là, mais des milliards sont investis dans l'informatique quantique. Aujourd'hui, un ordinateur quantique peut intégrer entre 100 et 1.000 qubits, ce qui les rend nettement plus puissants que les bits classiques. On estime qu'un ordinateur doté d'un million de qubits pourra casser les algorithmes existants.

Faut-il dès lors repartir de zéro ?

PRENEEL: Nous avons déjà commencé. Peter Shor a publié en 1994 un article où il explique comment un ordinateur quantique peut factoriser de très grands nombres et casser ainsi certains algorithmes cryptographiques. Et dans les années qui ont suivi, nous avons commencé à étudier des algorithmes capables de résister.

C'est ainsi que l'un de mes étudiants a fait en 2005 une thèse de doctorat sur ce thème, tandis que la première conférence sur la cryptographie post-quantique [le cryptage capable de résister à des ordinateurs quantiques, NDLR] s'est tenue en 2006 au département ESAT de la KU Leuven. A l'époque, entre 80 et 200 scientifiques se sont réunis pour analyser la situation et voir comment réagir. Entretemps, les pouvoirs publics américains ont mis sur pied une compétition dont les premiers résultats sont connus. En fait, ces algorithmes existent désormais.

« Quelque chose que j'ai contribué à créer en 1996 est intégré à chaque transaction bitcoin. Mais c'était impossible à prédire. »

Le défi pour les 10 prochaines années sera de migrer ces 50 milliards d'applications et de plateformes. Et c'est bien sûr un cauchemar. Tout le monde admet qu'il faut agir, mais aucun modèle commercial n'existe. Il est évidemment possible de migrer et de rendre donc vos systèmes sécurisés, mais les clés deviennent plus grandes, ce qui oblige à transmettre davantage de bits. Il faut donc tout revoir et adapter, pour en arriver finalement à quelque chose que vous aviez déjà. Dès lors, les pouvoirs publics vont devoir intervenir. On constate que certaines banques centrales et autorités publiques mettent la pression sur leurs entreprises, mais en pratique, il s'agit de plateformes extrêmement complexes. Une banque a des applications qui interagissent avec des dizaines de bases de données et de fournisseurs qui ont chacun leur propre agenda : il est impossible de tout changer d'un coup. Il faut aussi tenir compte du code dont on ne sait plus où le trouver.

On fait souvent la comparaison avec le Y2K, mais c'est beaucoup plus complexe. En 2000, l'Internet des objets n'existait pas et il n'y avait pas de milliards d'ordinateurs dans le monde. Aujourd'hui, on recense 30 milliards d'appareils qui possèdent chacun son propre système de mise en route avec des signatures, des navigateurs Web, des logiciels, etc. Il n'est pas question d'une simple mise à niveau, mais d'adaptation de la grande majorité des logiciels. C'est un défi énorme.

La KU Leuven a inauguré voici quelques semaines une chaire sur l'informatique quantique. Vous et ces professeurs sont-ils encore en phase ?

PRENEEL: L'entente reste très bonne. Cela peut évidemment paraître étonnant qu'une autorité publique investisse dans des applications destinées à craquer les systèmes actuels. Mais c'est en fait une sorte de course à l'armement. Si les Chinois y arrivent en premier, nous aurons un problème. Or l'informatique quantique a d'autres applications, notamment pour craquer la chimie ou la science des matériaux. En pratique, je ne pense pas qu'il y aura beaucoup d'ordinateurs quantiques pour craquer la sécurité. Si vous pouvez proposer un service capable de pirater les algorithmes des cartes d'identité, les autorités finiront par s'intéresser à vous. D'ailleurs, les autorités contrôlent désormais aussi les exportations de technologies comme les logiciels de piratage.

Comment entrevoyez-vous l'avenir, après des années à essayer de casser ou de protéger la sécurité ?

PRENEEL: Je suis quelque peu inquiet dans la mesure où nous sommes toujours plus dépendants de l'information. La société se digitalise très fortement. Du coup, les rapports de force évoluent. Celui qui détient le pouvoir décide de ce qu'il contrôle. Et si tout est numérique, tout peut aussi être davantage contrôlé. La cryptographie joue un rôle important à cet égard dans la mesure où elle permet de reprendre ce pouvoir et de rendre au citoyen une partie de ce contrôle.

Avec le Cosic, vous avez notamment piraté des Tesla. Y a-t-il d'autres projets dont vous êtes fier ?

PRENEEL: Voici 13 ans environ, nous →

avons lancé un projet sur la taxe kilométrique. Nous avions constaté que des villes comme Stockholm ou Londres avaient introduit ce système et commençaient à installer des caméras. Nous voulions une alternative qui soit plus soucieuse de la vie privée. Nous avons alors conçu une sorte de boîte noire intégrée dans le véhicule. Celle-ci enregistrait les déplacements et envoyait en fin de mois un message indiquant le nombre de fois que le conducteur était entré dans la zone de paiement. L'idée s'appuyait sur plusieurs aspects techniques pour empêcher toute désactivation du système par exemple. Mais tout avait été prévu et ce système avait selon moi 20 ans d'avance. En fait, nous avions démontré qu'il est possible de stocker des données en toute confidentialité tout en communiquant des informations pertinentes. Nous avions été capables de concilier vie privée et fonctionnalité.

Est-ce également ce que vous aviez essayé avec Coronalert [l'appli de traçage des contacts conçu et coordonné par Preneel durant la pandémie de Covid, NDLR] ?

PRENEEL: C'était une technologie similaire : tout stocker en local et ne centraliser qu'un minimum d'informations. L'Etat ne savait pas qui avait enfreint les règles et qui avait été en contact avec qui. En France par contre, l'autorité pouvait savoir qui avait trop circulé, mais pas en Belgique. Reste que presque personne ne le croyait. C'est évidemment un problème psychologique : les gens avaient l'impression que l'appli pouvait collecter leurs données et les communiquer à des tiers.

« La principale réussite de Coronalert est d'avoir pu débrancher l'appli par la suite. »

Je pense cependant que le principal succès à cet égard est que nous ayons pu désactiver l'appli. Nous craignions que les systèmes mis en place durant la pandémie, comme le Passenger Locator Form, continueraient d'exister. L'appli de détection des contacts avait d'ailleurs été conçu de manière à pouvoir débrancher simplement le serveur central. Chaque jour, les informations datant de plus de 40 jours étaient effacées des serveurs. Après 40 jours donc, c'était terminé. Il n'y a pas beaucoup de systèmes qui implémentent ce 'droit à l'oubli' de manière aussi automatique. Pas question d'avoir l'idée saugrenue de l'utiliser pour la grippe ou la rougeole. Si l'État veut à nouveau y songer, il faudra un nouveau cas d'usage. C'était l'un des critères de conception.

Vous craigniez les dérives ?

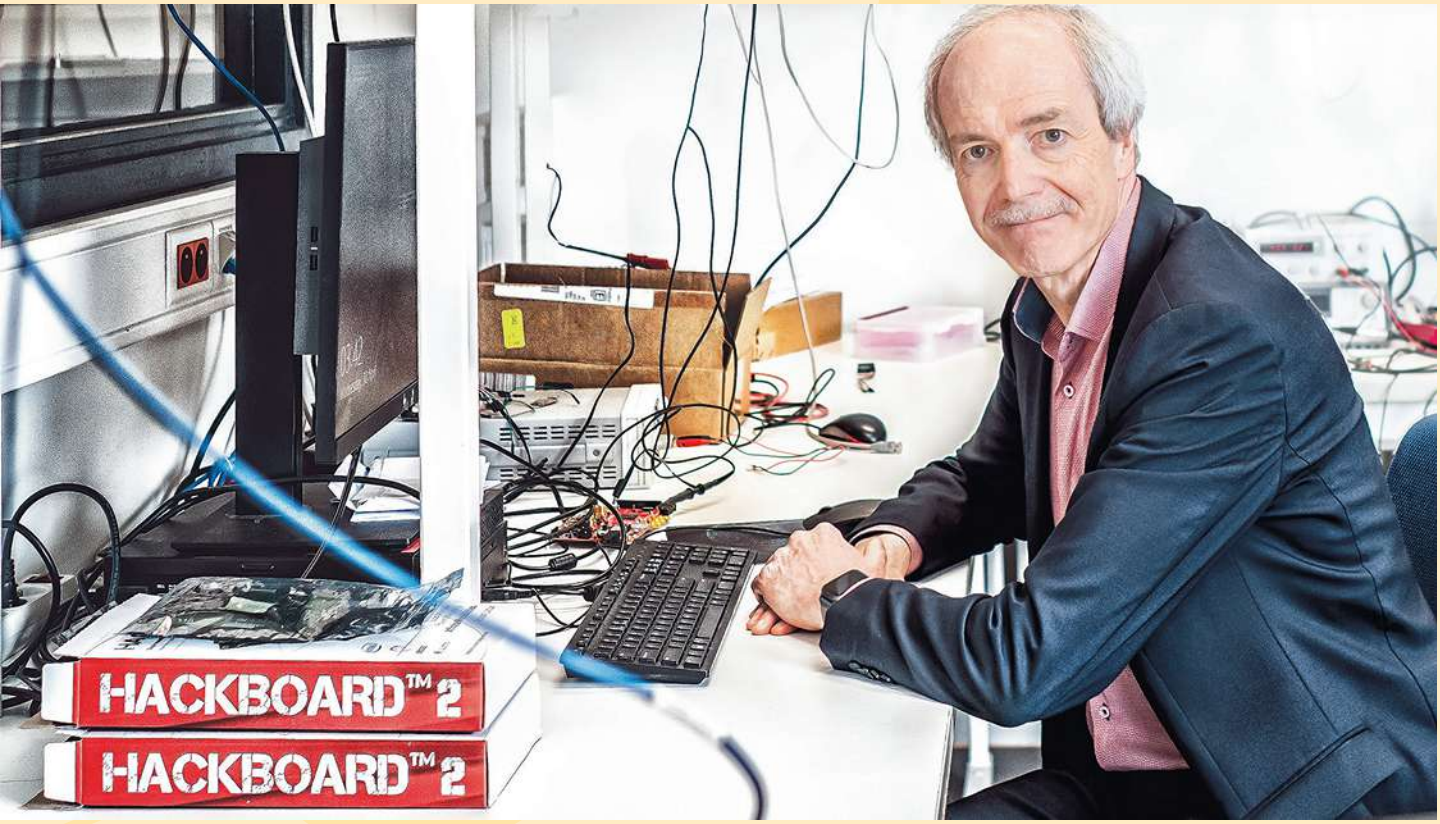
PRENEEL: Exactement. C'est un choix que nous avons fait en Belgique. Nombre d'autres pays ont par exemple intégré les codes de vaccination dans l'appli de traçage des contacts. J'ai demandé de ne pas le faire, car j'avais promis que les données des citoyens ne seraient jamais stockées dans l'appli. Cela étant, une appli de vaccination doit certes disposer de votre nom et de vos données, sans quoi il aurait été impossible de vérifier à la frontière que vous avez bien été vacciné. Du coup, l'autorité a développe une seconde appli. Il aurait certes été plus efficace de l'intégrer dans l'appli existante, mais une fois établi le choix de principe du respect de la vie privée, il fallait rester conséquent.

Vous vous posez souvent en défenseur de la vie privée et contre les tentatives du pouvoir de prévoir des portes dérobées pour accéder aux données. En a-t-il été ainsi de tout temps ?

PRENEEL: C'est récurrent. Le premier dossier dans lequel j'ai été plus ou moins impliqué concernait la Clipper Chip. Dans les années 90, le géant américain de la téléphonie AT&T avait lancé un téléphone à cryptage de bout en bout. L'entreprise entendait permettre aux hommes d'affaires de mener des conversations téléphoniques professionnelles renfermant des informations sensibles. L'administration Clinton entendait intégrer sa propre puce et même gérer les clés aux États-Unis. A l'époque, l'industrie et le monde académique s'y sont opposés. Cette Clipper Chip a finalement été arrêtée, mais l'autorité américaine de l'époque a étendu ses capacités d'interception.

Autre exemple : Apple contre le FBI concernant le stockage des téléphones. Le FBI avait demandé à Apple de pouvoir consulter le téléphone d'un terroriste, ce que celle-ci a refusé. Finalement, le FBI a dû renoncer, mais cela prouve que l'autorité cherche constamment une voie. Chez AT&T, il s'agissait de crime organisé et pour Apple de terrorisme. On pensait que le coupable n'attirerait pas les sympathies. Mais finalement, de tels dossiers risquent de servir de levier pour d'autres affaires en justice.

Les cas actuels concernent la pédopornographie ou le CSAM [Child Sexual Abuse Material, NDLR]. Il s'agit évidemment de matières très graves et les autorités comme Europol entendent pouvoir accéder à l'ensemble des communications en arguant de la protection des enfants. Dans ce domaine, il n'est en fait plus question de craquer



Bart Preneel: « Les révélations de Snowden ont été un premier rappel à l'ordre. »

le cryptage : on veut savoir ce qui se passe avant et après le cryptage. C'est par essence bien plus grave encore car ce 'client side scanning' peut aussi mener à des abus.

De quels ordres ?

PRENEEL: Pour l'instant, la pédopornographie est combattue par des hachages. Certaines organisations collectent ces contenus CSAM et ne vont évidemment pas les communiquer aux Google et Facebook de ce monde, mais bien les hacher. On mélange chaque image pour en faire un petit fichier et dès qu'une photo est postée sur Meta, on fait la même chose pour voir si ce hachage se trouve dans la base de données. Si tel est le cas, on peut retenir l'image. Mais ce système commence à atteindre ses limites. Les fonctions de hachage génèrent beaucoup de faux positifs et grâce à l'IA générative, il est possible de créer de nouvelles images qui ne seront pas détectées.

Par ailleurs, on s'intéresse toujours plus au 'client side scanning' étant donné qu'il y a de plus en plus de cryptage de bout en bout dans des services comme Signal ou WhatsApp et qu'il n'est plus possible d'intercepter la communication transmise. A la place, on utilise un logiciel pour regarder dans votre téléphone s'il y a des images CSAM. Notre souci est que, indépendamment du fait que cela ne fonctionne pas, il n'y a aucune transparence. Vous ne savez pas ce que contient la base de données qui vérifie votre téléphone. En d'autres termes, si Orbán par exemple veut savoir qui poste des mèmes à son sujet, il lui suffit d'ajouter des hachages à la base de données pour lui permettre de voir en temps réel qui sont les utilisateurs qui l'observent. Le problème est que l'on crée ainsi une sorte de super-outil pour dictateurs. Certes, il faut trouver une parade au problème du CSAM, mais il faut trouver une autre approche qui soit proportionnée et ne mette pas en péril la sécurité de chacun.

En faites-vous personnellement assez pour protéger votre vie privée ?

PRENEEL: Jamais assez à mon sens. Si vous avez un téléphone portable, vous savez que votre localisation est connue et mémorisée. Je vais certes éteindre plus souvent mon téléphone que d'autres ou le poser dans une autre pièce. De même, je suis prudent dans ce que je poste sur les médias sociaux. Cela étant, il faut être réaliste face à la fonction que j'occupe. Vous rencontrez de toute façon des étudiants, vous assistez à des congrès et des événements. Il y a des dizaines de personnes qui prennent des photos et qui communiquent tout ce que vous dites sur les réseaux sociaux. Il faut évidemment pouvoir continuer à vivre. →

La cybersécurité et le monde académique fonctionnent grâce à la collaboration internationale. Celle-ci est-elle désormais en danger, compte tenu de la situation géopolitique ?

PRENEEL: Je ne sais pas ce que nous réserve l'avenir. J'entrevois certes une tendance à une baisse de la collaboration. Je continue à collaborer avec la Chine et j'ai beaucoup d'étudiants étrangers, surtout chinois, indiens et iraniens. En soi, il s'agit là d'un enrichissement mutuel. Sur le plan économique, il y a pour l'instant beaucoup de compétition géopolitique, mais je pense que les scientifiques doivent continuer à collaborer. Durant la Guerre froide d'ailleurs, la collaboration entre scientifiques ne s'est pas arrêtée. C'est mieux ainsi car si l'on arrête de collaborer, l'étape suivante est d'en finir avec les publications, ce qui signifierait la fin d'une science ouverte. Si l'on travaille ensemble à la résolution de problèmes, cela va plus vite. Mais que se passe-t-il si chacun travaille dans son coin ? Dans le pire des cas, vous bénéficiez d'une légère avance, tandis que l'autre rattrapera son retard dès que vous aurez publié vos travaux. Qu'aurez-vous finalement obtenu ?

« Le défi pour les 10 prochaines années sera de migrer ces 50 milliards d'applications et de plateformes. Et c'est bien sûr un cauchemar. »

Sommes-nous en Europe trop dépendants de l'étranger sur le plan de la technologie et de la sécurité, et notamment des États-Unis ?

PRENEEL: Le sujet a pris de l'actualité avec le nouveau président, mais nous sommes depuis longtemps trop dépendants des USA. Il ne sera pas facile d'y remédier. Nous avons les cerveaux, nous avons les chercheurs et nous avons de plus en plus de start-up. Mais c'est surtout l'étape suivante vers les scale-up où l'Europe ne se montre pas assez dynamique. Il existe aussi de nombreuses frontières nationales, surtout en cybersécurité : une entreprise allemande éprouvera des difficultés à vendre ses produits en France et inversement.

Le second problème est le financement. On en trouve certes ici, mais avec le même plan d'affaires, vous trouverez 10 fois plus de fonds en Amérique. Il faut également faire d'autres promesses, mais ces fonds permettent de recruter immédiatement du personnel en marketing et d'accélérer les développements. Ici, tout va en revanche bien plus lentement.

L'UE a certes déjà pris certaines mesures.

PRENEEL: Un choix stratégique a été posé avec le Chips Act. Quant à savoir s'il s'agissait de la meilleure option, difficile de se prononcer. Mais pourquoi n'investit-on pas également dans les systèmes de gestion et les logiciels et matériels ouverts ? Dans la cybersécurité, on craint de trop dépendre des États-Unis, alors que toutes nos technologies IT sont en fait dépendantes des USA, de Taiwan et de la Chine. La cybersécurité ne peut s'aborder de manière isolée. On peut certes améliorer la sécurité de son cloud, mais si les grands acteurs du cloud ne sont pas européens, il reste toujours une limite au contrôle que l'on peut exercer. Certes, cela coûte énormément pour devenir indépendant. En fait, j'ai déjà eu de telles discussions lors des révélations de Snowden [qui, en 2013, avait fait fuiter des documents de la NSA indiquant que les États-Unis espionnaient les données à l'échelle mondiale, NDLR]. À l'époque, j'ai demandé aux entreprises d'y réfléchir, mais le sujet a été directement balayé. La technologie américaine était tellement supérieure. Si nous avions alors réagi à l'échelle européenne, la sécurité IT aurait peut-être été meilleure en Europe. Il s'agissait en fait d'un premier rappel à l'ordre face à une information qui devenait toute-puissante et à l'importance de celui qui en détient le contrôle.

Vous n'êtes certes pas encore retraité, mais quel regard jetez-vous sur votre carrière ? Où estimez-vous avoir eu de l'impact ?

PRENEEL: Je suis extrêmement chanceux d'être arrivé dans un secteur qui en était à ses balbutiements. J'ai pu trouver des personnes très qualifiées pour bâtir un groupe très performant. Si nous en sommes où nous nous trouvons, c'est en partie grâce au fait d'avoir pu trouver des collaborateurs très talentueux.

En tant que scientifique, je me suis beaucoup investi dans la création d'une communauté, tant au sein de la KU Leuven qu'en Belgique et à l'international. Entre 2004 et 2012, j'ai notamment dirigé un projet visant à intégrer l'ensemble des groupes de cryptographes en Europe, avec un agenda de recherche scientifique commun, des universités d'été et des ateliers. Ce faisant, nous avons pu regrouper des centaines de chercheurs. S'en est dégagée une culture de la collaboration dont l'impact a été énorme sur le secteur. En d'autres termes, si l'Europe a quelque peu avancé, c'est en partie parce que j'y ai contribué.

Els Bellens, photos Debby Termonia

L'an dernier également, les cubes de X-Treme Creations ont créé la sensation.

Comment X-Treme Creations magnifie les Data News Awards

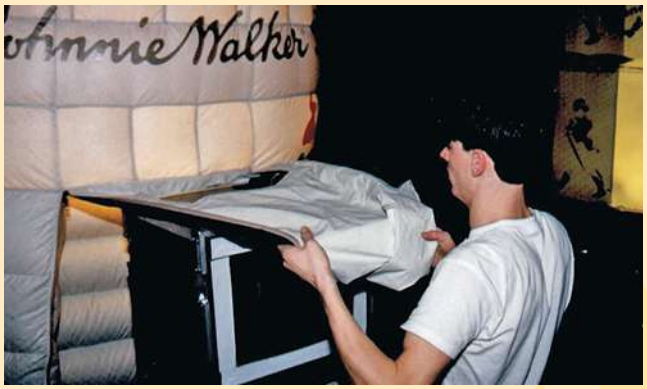
Les invités des Data News Awards for Excellence se souviennent certainement des grands cubes gonflables lancés dans le public. Voici comment l'idée a pris naissance.

Les objets gonflables sont désormais omniprésents lors de festivals et concerts, voire à l'occasion d'événements d'entreprise. Et même lors des Data News Awards donc. X-Treme Creations est à l'origine de ces dés de 1 m sur 1 m, imprimés à l'effigie des nommés au titre d'ICT Personality of the Year. Cela étant, l'histoire de X-Treme Creations remonte aux… châteaux gonflables. « Nous sommes en 1994 : à l'époque, la location et la vente de châteaux gonflables étaient relativement nouvelles. Mais désormais, cela fait partie intégrante de notre culture puisqu'on retrouve le château gonflable à pratiquement n'importe quelle fête d'anniversaire d'enfant », se souvient **Dan Vandevoorde**, fondateur.

Du château aux structures

L'expertise dans le gonflage de formes a rapidement incité Vandevoorde à se lancer dans un nouveau créneau inexploré. La rencontre avec un artiste espagnol qui avait travaillé pour la cérémonie d'ouverture des Jeux Olympiques de Barcelone en 1992 lui a ouvert la voie à des méga-événements. « Il s'agissait certes d'une niche que nous ne connaissions absolument pas », admet Vandevoorde. Le défi a été de convaincre une agence de publicité de se lancer dans l'aventure, d'autant que le potentiel des structures gonflables était à l'époque méconnu. « Ces 'inflatables' étaient alors synonymes de poupée gonflable. C'est d'ailleurs ce que nous avons eu mille fois comme réponse », sourit Vandevoorde.

L'un des premiers succès majeurs a été un piment gonflable pour Radio Donna en son temps, un succès qui a ouvert la voie à une collaboration avec de grandes marques. « Durant une dizaine d'années, nous avons créé tous les arcs-en-ciel de Red Bull à l'échelle mondiale. » De même, le monde des festivals, avec Tomorrowland comme important client depuis 2016, a découvert la puissance des imposantes structures gonflables réutilisables



Des ordinateurs portables gonflables aux arcs Red Bull, chaque projet est conçu sur mesure.

et durables puisqu'elles peuvent résister durant dix ans, voire davantage.

Références ICT mondiales

Dan Vandevoorde s'enthousiasme en évoquant la manière dont le textile, l'air et la créativité se rejoignent pour former un outil de marketing puissant, même dans le secteur ICT. « Lors du lancement de Windows 95 de Microsoft, nous avons conçu une dizaine, voire une vingtaine d'emballages de 4 m sur 6 m de haut. » De même, l'entreprise a fabriqué des structures gonflables pour Compaq, Nokia, Salesforce –« Nous avons fabriqué un Trailblazer pour l'un des plus grands salons en Allemagne. » et même Apple aux débuts de l'entreprise.

Cubes

Chaque projet est conçu sur mesure, et notamment nos dés. « Nous devons savoir d'emblée à quoi va servir la structure gonflable, à quelle application concrète elle servira. Pour vos Awards, le projet était précis : des 'crowd cubes' qui devaient être lancés parmi les invités, précise Vandevoorde. En concertation avec vos équipes, nous avons défini les dimensions, le nombre de pièces et le type d'impression. »

Le concept en tant que tel est en général imaginé par le client ou son agence de publicité. « Celle-ci connaît son client et sait ce qu'il désire, poursuit Vandevoorde. Ainsi, vous nous avez présenté un design très professionnel. Cela étant, les agences de pub – ce que nous appelons le marché intermédiaire – nous fournissent désormais aussi des idées très élaborées. »

« X-Treme Creations se concentre sur la réalisation technique. Les cubes sont d'abord cousus et testés pour leur étanchéité à l'air avant d'être recouverts de la housse imprimée. Le travail de couture se fait en partie dans nos propres ateliers et en partie centralisés chez des couturières professionnelles », précise encore Vandevoorde qui gère l'entreprise en compagnie de son épouse, Suyin Aerts. Ensemble, ils continuent à innover et desservent désormais, outre le secteur de l'événementiel et du marketing, des marchés de niche comme les congrès de médecine et même des événements spéciaux pour les vétérinaires. « Ce n'est pas toujours de la technologie de pointe », admet Vandevoorde lorsqu'il évoque le processus de production. Mais la transposition d'un concept en une réalisation en 3D sur une dimension de 1, 5 ou 10 m n'exige pas seulement une maîtrise technologique, mais aussi énormément d'expérience. » Et le résultat, certainement dans le contexte adéquat associant musique et public, se révèle impressionnant.

Kristof Van der Stadt