Business Magazine

U&US

By Telindus

Proximus House

Un levier pour la croissance et l'innovation

European Space Agency

Pushing the frontiers of cybersecurity

Blockchain

Shaping the future of trust

More inside

#9

EMERGING TECHNOLOGIES

HOW TO BUILD A PROSPEROUS AND SAFE FUTURE?

U&US #9

Chers amis,

Cette 9ème édition du Magazine U&US vous propose un tour d'horizon des technologies qu'il faut adopter aujourd'hui pour évoluer dans l'économie de demain.

Intelligence Artificielle, Machine Learning, Big Data, Blockchain, Internet des Objets... Il ne s'agit plus de prospective, nous sommes définitivement entrés dans l'ère de la Data-Driven Economy. Au sein des entreprises de toutes tailles, de nouveaux métiers émergent : Chief Analytics Officer, Data Scientist, Data Engineer, ou encore Data Protection Officer. Les start-ups développent quant à elles des solutions utilisant l'IA, la Blockchain ou l'IoT pour proposer des services toujours plus innovants.

Ces technologies sont déjà exploitées au quotidien par des applications telles que la reconnaissance vocale, les recommandations musicales, la prévision d'achat, la détection des fraudes et les assistants virtuels comme Cortana, Siri ou Alexa.

Et nombre d'entre vous, dans la finance ou dans l'industrie, ont d'ores et déjà déployé des solutions métier qui exploitent une partie de l'énorme potentiel de ces technologies émergentes.

Cependant, tout phénomène de transformation comporte sa part de risque et, au cours des années à venir, les menaces liées à la cybersécurité continueront à faire planer une inquiétude sur l'économie mondiale.

À leur manière, beaucoup de cybercriminels sont des défricheurs de nouvelles technologies. Leurs succès dans le domaine du ransomware, par exemple, montrent qu'ils opèrent déjà parfaitement à l'échelle mondiale. Ils exploitent les capacités d'analyse aujourd'hui disponibles pour toucher un grand nombre de victimes de petite taille. Ces pionniers de la cyberdélinquance avancée tirent autant d'avantages de la révolution numérique que les entreprises dont ils se nourrissent.

La protection contre ces menaces nécessite une approche proactive, intégrée et automatisée de la cybersécurité. Aujourd'hui, les experts en cybersécurité ont complété leur arsenal défensif par des outils tirant parti de l'IA et du Big Data. La capacité de ces technologies à détecter précocement les signes avant-coureurs d'attaques et les menaces potentielles ouvrent la voie à une cybersécurité prédictive, créatrice de valeur et pilotée par des analystes aux capacités renforcées.

En vous souhaitant une excellente lecture

GÉRARD HOFFMANN

CEO, Proximus Luxembourg

SOM-MAIRE

U&US #9

PROXIMUS LUXEMBOURG S.A.
18, rue du Puits Romain
Z.A. Bourmicht 8070 Bertrange
Tél :+352 450 915-1

GESTION ÉDITORIALE
Michaël Renotte

PHOTOGRAPHIES
Loris Romano

CONCEPTION GRAPHIQUE
Deuux

IMPRESSION
1000 exemplaires

POUR ÉCRIRE À LA RÉDACTION
marketing@telindus.lu

@ telindustelecom
/Telindus-luxembourg
/Telindus_lu

DEGROOF PETERCAM

S'ASSOCIE À TELINDUS

Luxembourg, le 19 novembre 2019 – Degroof Petercam s'associe à Telindus Luxembourg, la marque dédiée au marché professionnel de Proximus Luxembourg, pour moderniser son infrastructure ICT au Luxembourg et en Belgique et s'appuyer sur des services managés associés.

Afin de soutenir ses ambitions stratégiques sur le long terme, Degroof Petercam a décidé de moderniser son infrastructure pour assurer un environnement ICT flexible et durable.

Cette initiative s'inscrit dans le cadre du programme de transformation numérique du groupe qui s'étend sur plusieurs années et couvre quatre aspects majeurs : Infrastructure, Applications, Processus et nouvelles méthodes de travail.

Degroof Petercam bénéficie des dernières innovations déployées par Telindus sur son infrastructure d'hébergement "U-Flex", la solution phare de cloud privé de Telindus pour l'hébergement des infrastructures clients à grande échelle. Elle offre des combinaisons flexibles de solutions d'hébergement, d'infrastructures dédiées et mutualisées ainsi que de nombreux services opérés et supervisés 24h/24 et 7j/7, tels que les services managés de sécurité mais aussi des solutions traditionnelles d'entreprise comme les services de messagerie, de collaboration ou de téléphonie.

Les datacentres de Degroof Petercam seront centralisés au Luxembourg, pour les entités de Belgique et de Luxembourg dans un premier temps. Proximus Luxembourg exploitera l'infrastructure cible, tout en y déployant des technologies de pointe éprouvées. Fort de son expertise, Proximus Luxembourg accompagnera le groupe dans les développements futurs des technologies de cloud computing, en ligne avec les ambitions de Degroof Petercam.

DE GAUCHE À DROITE :

Yvan Pirenne
Group CIO de Degroof Petercam

Sylvie Huret
CFO de Banque Degroof Petercam Luxembourg

Pascal Nyckees
Ex-Group COO de Degroof Petercam

Bart Van den Meersche
Chief Enterprise Market Officer de Proximus Group

Bruno Houdmont
CEO de Banque Degroof Petercam Luxembourg

Christian Haux
Chief Enterprise Market Officer de Proximus Luxembourg

"Proximus Luxembourg a su se différencier par son offre d'externalisation intégrée qui répond à nos besoins opérationnels, à nos standards de sécurité de haut niveau et à nos fortes ambitions en matière d'innovation. De plus, le passage de nos anciens serveurs énergivores à des serveurs externes écologiques ultramodernes nous permettra de limiter notre impact sur l'environnement", déclare Pascal Nyckees, Ex-Group COO de Degroof Petercam.

Bart Van den Meersche, Chief Enterprise Market Officer de Proximus Group, se réjouit : "Nous sommes extrêmement fiers d'avoir été choisis par Degroof Petercam au terme d'un processus de sélection rigoureux. Nous nous engageons pleinement à leurs côtés pour réaliser leurs projets d'avenir en termes d'innovation et de croissance."

Gérard Hoffmann, CEO de Proximus Luxembourg, conclut : "Avec Degroof Petercam, nous partageons les mêmes valeurs. Ensemble, nous innovons, ce qui est vital pour un pays comme le Luxembourg dont l’économie repose en large partie sur les services."

Le projet a été lancé officiellement le 14 novembre dernier au siège de Banque Degroof Petercam Luxembourg, lors d’une cérémonie de signature qui a réuni la direction des deux sociétés.

MICROSOFT TEAMS DIRECT ROUTING

Launched in 2017, Microsoft Teams could become the N°1 platform for corporate collaboration and communication as from 2020[1]. The recent addition of the Direct Routing feature to Microsoft Teams gives Telindus experts the opportunity to summon the full range of their talents, from IT to telecom.

Mathieu Gillet, *Sales Consultant at Telindus*

[1] *Spiceworks, Spiceworks Study Reveals Adoption of Microsoft Teams is Accelerating in the Workplace, 10 décembre 2018*

Microsoft Teams is expected to shortly replace Skype for Business. In the meantime, the Teams platform has already convinced 500,000 organizations around the world[2], breaking the record for the fastest growing business application in Microsoft history[3]. "The reason for this success is due to a real need for companies to have an efficient multi-channel collaboration platform, able to centralize information but also to keep track of all exchanges", explains Mathieu Gillet, Sales Consultant at Telindus. "At a time when home office and mobility are gaining ground, remote work is becoming more widespread, and newly fragmented teams need to find ways to collaborate and co-publish despite the physical distance", he says.

Integrating telecoms and collaboration in one same platform

For businesses to realize the full potential of their platform, the Redmond firm relies on partners with multiple skills, like Telindus, able to aggregate the different types of content produced by companies in an integrated collaboration space. "Microsoft Teams is a collaborative cloud platform that provides access to all essential corporate features in one single platform: instant messaging, threads, storage and sharing of resources, audio and video calls, meetings, planning and schedules, or working groups", summarizes Mathieu Gillet. "With the addition of Direct Routing to Microsoft Teams and by leveraging its own systems integrator and telecom operator activities, Telindus now allows businesses to make and receive calls with their landline phones through the Teams platform, based on their existing equipment", he adds.

A versatile shared workspace

At the crossroads between collaborative solutions and telecommunication, Microsoft Teams makes it possible to collect information, structure content and store it in a way that it can be easily retrieved and accessed. "These contents include conventional telephone conversations, videoconferencing or chat with link sharing", Mathieu Gillet says. Teams users can for instance record a meeting, have it automatically transcribed as text via an AI-based transcription application, and store it on a SharePoint team site created for the occasion". Video and audio files can be searched based on their content and not just by their file name, which results in a more relevant search. "This can be very useful in the context of a support service, a commercial service, or in a regulatory context when it comes to finding the name of a person or a brand mentioned in different conversations", he adds.

An ecosystem of solutions

Taking advantage of the great flexibility offered by Microsoft Teams, Telindus leverages its multiple skills to offer businesses an ecosystem of solutions covering a wide range of activities: strong authentication system for mobile devices to control access to data stored in the cloud, training-related recording solution for call centers, or segregation of exchanges between departments to prevent conflicts of interest (ethical wall). "These are complete solutions built around Microsoft Teams with different partner solutions", says Mathieu Gillet. "Our goal is to make the Microsoft Office 365 platform the ideal tool to help our customers be successful with their digital transformation, from small businesses to large corporations."

Orchestrating the various skills

"It is usual for us to encounter totally heterogeneous environments: telephone services with one provider, videoconferencing with another, instant messaging with a third one", says Mathieu Gillet. "This is an opportunity for us to demonstrate our creativity and our sense of innovation by interconnecting these components of various origins and, as a result, consolidate the user experience."

With 700 employees, Telindus has industry-leading capabilities in systems integration, an activity that requires mobilizing and orchestrating many different businesses. "It is precisely this cohesive force that allows us to provide businesses with effective and easy to use solutions", says Mathieu Gillet. "But isn't it characteristic of experts to simplify for the customer something that is intrinsically complex?", he concludes.

[2] *Microsoft, Microsoft Teams wins Enterprise Connect Best in Show award and delivers new experiences for the intelligent workplace, 19 mars 2019*

[3] *Microsoft, What's new in Teams - Microsoft Ignite Edition, 24 septembre 2018*

TELINDUS: FIRST GOOGLE CLOUD PARTNER

IN LUXEMBOURG

Google Cloud

Luxembourg December 2nd, 2019 – Telindus is proud to announce its partnership with Google Cloud to deliver secure business solutions encompassing the full range of infrastructure and platform as a service products of Google Cloud. Those include Big Data platforms, Data Analytics or Machine Learning services, to name a few, which are offered both fully native and in hybrid mode to the Luxembourg market.

As first Google Cloud partner in Luxembourg, Telindus will address the digital transformation needs of its customers and power comprehensive, integrated and secured solutions that fits the financial sector as well as the industry and public sectors.

“We are very excited about this partnership with Telindus in Luxembourg. There is a very high growth of Cloud services in the European market and partnerships are a key catalyst of this growth. This partnership will help Google accelerate in an important market as Luxembourg", says Edward Boute, Head of Google Cloud Belux.

With this partnership, Telindus aims at supporting its customers to build innovative ICT infrastructures, which are capable to efficiently transform customer businesses using on-premise and cloud environments. Google is the perfect match for such hybrid deployments since most of its managed products are also released as open-source projects, e.g. Kubernetes. Google cloud even simplifies further hybrid deployments and their management, based on the April 2019-released hybrid Kubernetes platform called Anthos.

In general, Google’s openness allows to control and monitor tightly cloud usage, whilst allowing customers to take leverage of Google’s innovative pace. Google also proposes some interesting tools for big data projects, e.g. BigQuery- as well as the required data processing and analytical tools are exposed to customers to allow them to take leverage of those data storage and processing strengths for their own projects at petabyte-scale…

“We are delighted to make this partnership happen with Google Cloud to accelerate the adoption of its leading technologies at our customers", says Jacques Ruckert, Chief Solutions & Innovation Officer at Telindus. “The partnership is already gaining first momentum using key strength of the Google Cloud. Several projects have been meanwhile successfully delivered on top of Google Cloud.”

Artificial Intelligence

Google is well known for its capabilities with regard to artificial intelligence. Therefore, a customer decided to improve its customer support using the chatbot capabilities of Google Cloud called Dialogflow. Using such technology on its webpage will reduce the amount of service requests to be handled manually at the helpdesk and decrease response time to the customer.

Software Development in the cloud (CI/CD pipelines)

Telindus is running multiple software development projects using Google Cloud for itself or for its customer projects. Telindus flagship fintech application called DigitalKYC is one example of those. For such purposes Google Cloud allows to efficiently manage the end-2-end software development lifecycles, such as software build, release and versioning with strong integration and container based hosting on top of Kubernetes.

Big Data

First Big Data projects have been implemented on top of Google Cloud using their data ingest, transformation pipelines and dataware-housing solutions, which are capable to gain real-time insights into petabyte-scale datasets using machine learning, artificial intelligence and analytics on them.

PROXIMUS HOUSE

UN LEVIER POUR LA CROISSANCE ET L'INNOVATION

C'est le 27 juin 2019 que s'est déroulée l'inauguration officielle du nouveau siège de Proximus Luxembourg, "Proximus House", en présence du Premier ministre Xavier Bettel et de Dominique Leroy, Ex-CEO du Groupe Proximus. Après la fusion de Tango et Telindus le 1er janvier de cette année, cet événement consacrait aussi la réunion des deux entités sous le même toit.

Près de 500 invités – clients, partenaires, mandataires publics, personnalités académiques et acteurs économiques – s'étaient joints aux directeurs et collaborateurs de Proximus Luxembourg pour célébrer à la fois les 20 ans de Tango, le 40ème anniversaire de Telindus et l'inauguration du nouveau bâtiment. "Cela fait plus de 10 ans que nous recherchions le site idéal pour rassembler dans un même lieu tous nos collaborateurs et l'ensemble des activités qu'ils mènent", a confié Gérard Hoffmann, CEO de Proximus Luxembourg. "Nous étions jusqu'ici partagés entre nos installations de Bertrange, de Strassen et d'Esch-sur-Alzette. Aujourd'hui, sur ce site de Bourmicht, nous inaugurons un nouveau bâtiment de 20.000 m^2 qui va nous permettre de développer une culture d'entreprise commune au service d'une stratégie ambitieuse."

Un rôle moteur en matière d'innovation

Proximus Luxembourg a pour objectif de devenir le n°1 du marché national en termes d'innovation. En témoignent les premières connexions 5G au Luxembourg déployées précisément par la firme de Bourmicht. "En tant qu'acteur de premier plan à la fois sur les marchés ICT et Télécom", a ajouté Gérard Hoffmann, "nous avons à cœur de poursuivre notre contribution à l'accélération de la digitalisation du Luxembourg à travers le développement de la connectivité, d'infrastructures résilientes, de la 5G, mais aussi de technologies innovantes comme le cloud hybride, l'IoT, la FinTech, la Blockchain, l'Intelligence Artificielle et le Machine Learning."

Le CEO de Proximus Luxembourg a rappelé que, depuis plusieurs décennies, les gouvernements successifs s'étaient montrés visionnaires en soutenant activement les secteurs de l'ICT et des Télécoms. Il a ainsi évoqué "la libéralisation des marchés des télécommunications, à l'aube du millénaire, qui a conduit à la naissance de Tango" ainsi que "la création de LuxConnect par le gouvernement en 2006, un événement clé qui a marqué un changement de paradigme pour tout le secteur de l'ICT au Luxembourg dont la croissance s'est accélérée de manière formidable par la suite."

Data-driven economy

Gérard Hoffmann a également salué la nouvelle stratégie d'innovation pour une Data-Driven Economy, présentée en mai dernier par le Premier ministre, Xavier Bettel, et par le ministre de l'Economie, Etienne Schneider. "Le gouvernement luxembourgeois reconnaît ainsi la place centrale que l'ICT occupe dans le développement économique global. Par-là, le gouvernement contribue également à remettre l'Europe sur la carte mondiale de la technologie en incitant le secteur à participer à la course aux applications de l'Intelligence Artificielle, pour laquelle tout reste encore ouvert", a-t-il déclaré.

> “ Ce nouveau bâtiment nous permettra d'inspirer la communauté et de favoriser les échanges et l'émulation, ainsi que de mieux recruter des jeunes passionnés de technologies qui recherchent un environnement créatif et convivial.
>
> **Gérard Hoffmann, CEO de Proximus Luxembourg**

Le CEO de Proximus Luxembourg a conclu son intervention en affirmant la volonté de l'entreprise de poursuivre sur la voie de l'innovation en demeurant la référence dans les services technologiques de pointe. "En ligne avec les objectifs digitaux de notre gouvernement, nous investissons dans les technologies et les infrastructures d'avenir", a-t-il dit.

Des ambitions partagées

Dominique Leroy, Ex-CEO du Groupe Proximus, a confirmé que cette volonté était partagée par la maison-mère de l'entreprise luxembourgeoise. Elle a d'ailleurs rappelé les liens forts qui unissent le groupe au Luxembourg, "un pays dynamique et précurseur à bien des égards, dont les initiatives inspirent ses voisins d'Europe et, notamment, la Belgique".

L'inauguration du nouveau bâtiment de Proximus Luxembourg marque, selon elle, "l'engagement du groupe à soutenir le développement du secteur au Luxembourg. Nous avons déjà pu observer les premiers effets bénéfiques des synergies entre l'univers des télécommunications et celui de l'ICT à travers le rapprochement de Telindus et Tango", a constaté Dominique Leroy.

Renforcer le tissu digital

L'engagement du Groupe Proximus sur le marché luxembourgeois a été démontré par la participation de celui-ci au développement des infrastructures de télécommunication au Luxembourg, dont les services sur la fibre, la téléphonie mobile ou encore par son soutien commercial à l'implantation de Data Centres de dernière génération par LuxConnect. "Au cours des cinq dernières années, nous avons investi près de 100 millions d'euros dans nos infrastructures", a déclaré Dominique Leroy.

Le Groupe Proximus contribue également au développement de l'écosystème digital luxembourgeois, notamment par sa participation à la Luxembourg House of Financial Technology ou encore à travers son investissement dans le Digital Tech Fund, un fonds d'amorçage créé par le gouvernement et un groupe d'investisseurs privés pour soutenir le financement des start-ups luxembourgeoises en phase de démarrage.

Dominique Leroy a encore souligné que si Proximus Luxembourg se plaçait aujourd'hui parmi les plus grands acteurs sur son marché, l'entreprise contribuait également à la vigueur du groupe. "Les projets développés ici autour du cloud computing ou de la 5G – dont le déploiement aura vraisemblablement lieu avant la Belgique - seront mis à profit plus largement sur tous nos marchés. Dans des domaines d'innovation comme celui de la Blockchain, dont le potentiel est encore trop peu exploité, ou encore de la FinTech, Proximus Luxembourg est précurseur dans le groupe", a-t-elle affirmé.

Faire ensemble du Luxembourg une smart nation

Premier ministre et ministre des Communication et des Médias, Xavier Bettel est également à la tête du nouveau ministère de la Digitalisation, créé il y a quelques mois pour mettre en œuvre les ambitions numériques du gouvernement. Il a lui aussi souligné les liens forts qui se sont forgés entre Le Luxembourg et le Groupe Proximus. Xavier Bettel a rappelé le rôle de Telindus et de Tango dans le développement de l'économie et de la société luxembourgeoises, ainsi que dans la digitalisation du pays. "Telindus et Tango ont non seulement fortement marqué l'histoire industrielle de leurs secteurs mais continuent de façonner l'avenir", a-t-il déclaré. "L'engagement des dirigeants de Proximus Luxembourg dans les associations professionnelles pour travailler dans l'intérêt général du développement du secteur est remarquable. Par la mobilisation de leurs meilleures compétences et de leurs réseaux à l'échelle internationale, ils contribuent également à développer avec vigueur la stratégie du secteur. Je n'en veux pour preuve que les voyages d'étude que Gérard Hoffmann organise avec la Fédération des Industriels Luxembourgeois depuis de nombreuses années à l'attention du secteur ICT et auxquels participent activement des représentants du secteur public. Ces expériences communes ont trouvé leur répercussion dans notre stratégie", a rappelé Xavier Bettel.

> “ J'ai la chance d'être le Premier ministre d'un pays où nous pouvons compter sur les acteurs privés.
>
> **Xavier Bettel, Premier ministre du Grand-Duché de Luxembourg**

"Il est essentiel d'œuvrer ensemble pour faire du Luxembourg une Smart Nation", a encore insisté le Premier ministre. "Les citoyens, les sociétés telle que Proximus Luxembourg, travaillent main dans la main avec le gouvernement pour amener ce pays aux avant-postes de l'innovation".

Innover pour le bénéfice de tous

Confirmant les propos de Gérard Hoffmann et Dominique Leroy, Xavier Bettel a souligné que le Luxembourg était l'un des premiers pays à s'être donné une vaste stratégie en matière de 5G et à avoir élaboré les premiers projets pilotes. "En tant qu'homme politique, je suis un fervent défenseur de la place digitale luxembourgeoise", a-t-il affirmé. "Je veux que nous soyons les premiers à mettre en œuvre de manière concrète la technologie 5G. Mais je veux aussi que chacun en comprenne les enjeux. Nous allons donc continuer nos efforts pour nous assurer que toutes les parties de la population bénéficieront de ces progrès. Tout le monde doit avoir les compétences nécessaires pour profiter de ces développements. Elles doivent devenir des compétences de base pour des technologies qui feront partie de notre quotidien", a déclaré le Premier ministre.

> “ En tant qu'homme politique, je suis un fervent défenseur de la place digitale luxembourgeoise. Je veux que nous soyons les premiers à mettre en œuvre de manière concrète la technologie 5G et que cela profite à chacun.
>
> **Xavier Bettel, Premier ministre du Grand-Duché de Luxembourg**

Guidé par la volonté de faire du pays une des forces motrices de l'ère digitale, le Luxembourg investit également des moyens importants dans l'éducation et la formation. "Nous avons beaucoup investi - et nous continuons à investir - dans l'éducation et la formation professionnelle. Nous venons ainsi de lancer, de concert avec les professionnels de l'ICT, une initiative pour permettre aux personnes qui se trouvent sur le marché de l'emploi de rebondir et à celles qui ne possèdent pas de formation spécifique de se former aux technologies du digital", a expliqué Xavier Bettel.

"Pourtant, lorsque je considère le développement que connaît l'économie digitale en Asie et aux Etats-Unis, je ne peux que constater qu'en Europe, nous avons encore du retard. Nous devons être plus actifs", a-t-il averti. La mise en œuvre du plan d'action "Digital Lëtzebuerg" et la promotion du secteur ICT restent donc une priorité pour le gouvernement luxembourgeois, tout comme la mise en œuvre de stratégies nationales dans les domaines de l'intelligence artificielle, de l'innovation basée sur les données, de l'internet des objets et de la 5G. "Le Luxembourg a l'ambition de devenir l'une des sociétés digitales les plus avancées au monde, et tout particulièrement dans l'Union Européenne. Ce n'est qu'ensemble que nous pourrons y parvenir, en unissant les forces du secteur public à celles des entreprises privées", a conclu le Premier ministre.

Proximus Luxembourg, née de la fusion en janvier 2019 de Telindus et de Tango, est une filiale du **Groupe Proximus**, une entreprise qui compte aujourd'hui 13.000 salariés. Proximus est principal fournisseur de services de téléphonie, d'internet, de télévision et de services ICT en Belgique.

Proximus Luxembourg rassemble les marques commerciales Tango et Telindus sous une même enseigne et emploie 700 collaborateurs, au service de 1.800 entreprises et 280.000 clients privés. Les deux marques opèrent conjointement afin de répondre à tous les besoins en télécommunication des clients particuliers et professionnels au Luxembourg. Tango propose des services de téléphonie fixe et mobile, d'internet et de télévision aux particuliers et aux petites entreprises. Telindus fournit pour sa part des services ICT et de télécommunications fixe et mobile aux moyennes et grandes entreprises ainsi qu'aux administrations publiques.

Fondée en 1979, **Telindus Luxembourg** accompagne toutes les entreprises et les administrations publiques dans leur transformation digitale en leur fournissant des solutions ICT et télécoms holistiques ainsi que des services de support sur mesure. Ses domaines d'expertise comprennent les télécommunications fixes et mobiles, les infrastructures ICT, le multicloud, les solutions FinTech, la cybersécurité et les services managés. Grâce à son Training Institute, Telindus répond à l'ensemble des défis de ses clients et permet aux professionnels de rester à la pointe en matière de meilleures pratiques et technologies ICT.

Tango est présente sur le marché luxembourgeois depuis 1998. Premier opérateur alternatif du pays, Tango propose un large portefeuille de produits incluant des services de TV, internet, téléphonie fixe et mobile aux clients résidentiels et petites entreprises. Proche de ses clients, elle s'appuie sur l'efficacité de son service clients et un réseau de distribution comprenant 11 points de vente Tango et 16 points de vente partenaires. Tango s'entoure également de partenaires internationaux tels que Vodafone, pour garantir à ses clients une expérience de communication optimale, même à l'étranger.

Proximus House accueille 700 employés sur une superficie totale de 19.500 m^2, dont 10.000 m^2 de bureaux. Les espaces ont été spécifiquement conçus pour favoriser la collaboration entre employés, tout en permettant l'émergence d'une nouvelle manière de travailler. Le principe du flex desk, par exemple, apporte davantage de flexibilité et de mobilité aux employés en leur permettant de s'installer en équipe et par projet, plutôt que dans des espaces préétablis. Des espaces modulables et des silent spaces ont également été mis en place.

Ce nouveau bâtiment prend en compte le bien-être des collaborateurs, avec notamment la mise en place de plusieurs espaces de détente (coffee corners, cafétéria, etc.) et d'espaces de réunion informels.

De réelles initiatives pour l'environnement ont également été développées : un éclairage intelligent pour chaque bureau afin d'économiser l'énergie, des stores automatisés pour favoriser la lumière naturelle et mieux réguler la température du bâtiment, ou encore un parking incluant des espaces dédiés aux vélos pour favoriser la mobilité douce. De plus, les employés sont encouragés à opter pour le covoiturage. Du clean desk au paperless policies, en passant par le recyclage encouragé dans tous les espaces de travail, Proximus House fait la part belle à l'environnement.

L'objectif principal de toutes ces innovations est de permettre aux employés de travailler de manière plus efficiente, que ce soit individuellement ou en équipe. Parce que des ambitions fortes ne peuvent se réaliser qu'avec des équipes fortes.

EMERGING TECHNOLOGIES

BY GARTNER

The digital age requires a new risk and security mindset

In the digital age, security is an integral part of the digital business equation. Data protection is evolving to include emerging technologies such as artificial intelligence and machine learning, blockchain, OT-IT convergence, advanced analytics, and the pervasive presence of mobile, cloud and the internet of things. These technologies are bringing new opportunities, as well as new risks and challenges.

According to Robert Handler[1], research vice president and distinguished analyst at Gartner, "As most industries evolve, their risk management approaches fail when they encounter previously unknown hazards. In an IT context, digitalization represents a point of rapid evolution, and it will create new risks".

The digital world is ever more complex, increasing the importance of risk management. While it is impossible to know the specifics of how or when an unknown risk will become reality or what its impact will be, we can foresee some factors that lead to new risks.

"Digitalization magnifies risk", Robert Handler explains. "Digital projects connect more and more things together, many of which are not within the direct control of the project leaders." This trend adds complexity and interdependency to organizational systems, sometimes in an exponential way. The current need for speed environment of digital business discourages redundancy. Therefore, potential points of failure proliferate and fragility rises.

> “ Multiple small points of failure can cascade into more-serious business risks.

"This complexity will accelerate as we connect 5.5 million new things a day to the internet of things", adds Robert Handler. "Even without that, many IT organizations are already struggling with their focus being limited to their internal systems."

An adaptive approach

Gartner advises security experts to apply a new approach - called CARTA (Continuous Adaptive Risk and Trust Assessment) by the firm - to stay competitive with emerging business opportunities. The key is to apply the philosophy across the business from DevOps to external partners.

"We need security that is adaptive everywhere to embrace the opportunity - and manage the risks - that come with this new digital world, delivering security that moves at the speed of digital business", says Neil MacDonald[2], vice president and distinguished analyst.

[1] *Smarter With Gartner, Revisit Risk in the Age of Digital Transformation, Gartner*

[2] *Smarter With Gartner, The Gartner IT Security Approach for the Digital Age, Gartner*

Data analytics need to be a standard part of the arsenal. Despite the hype about big data, companies can derive real value from machine learning. "Anomaly detection and machine learning are helping us to find bad guys that have otherwise bypassed our rules-based prevention systems", says Eric Ahlm, research director at Gartner. "That's why analytics are so relevant to security operations today, they are good at finding bad guys in the data that other systems missed."

The average time to detect a breach globally is 197 days and the average cost is $3.86 million, according to the Ponemon Institute Cost of a Data Breach Study 2018[3]. Analytics will speed up detection, and automation will speed up response time, acting as a force multiplier to scale the team without adding people. Analytics and automation ensure enterprises focus limited resources on events with the highest risk and the most confidence.

For access protection in the digital world, companies must be constantly monitoring. One time authentication is fundamentally flawed when the threat is past the gate. For example, if a user is downloading sensitive data to a device. The data should be encrypted with digital rights management before it's downloaded, and then the user should be monitored. If he starts to download too much, throttle access or raise an alert for investigation.

When it comes to DevOps, security needs to start early in development and identify issues that represent a risk to the organization before they're released into production. Modern applications are not developed, but rather assembled from libraries and components. Scan the libraries for known vulnerabilities and eliminate the majority of the risk. For custom code, balance the need for speed with the need for security.

> “ By 2025, Machine Learning will be a normal part of security practice and will offset some skills and staffing shortfalls.[4]

Finally, ecosystem partners add new business capabilities, and new security complexities.

"Risk management is no longer the domain of a single enterprise and it must be considered at ecosystem level", Eric Ahlm explains. "The success of my product or service is now fundamentally intertwined with others. My risk is their risk. Their risk is my risk. It's one in the same."

[3] *Ponemon Institute, 2018 Cost of a Data Breach Study, IBM*

[4] *Smarter With Gartner, Top Security and Risk Management Trends For 2018*

The Future of AI Technologies

The strategic application of Artificial Intelligence has the potential to generate game-changing outcomes. However, AI adoption has increased nearly threefold since 2017, raising the chances of misaligned core technologies and AI initiatives. Gartner has been tracking AI trends and, in November 2018, the firm identified five strategic planning assumptions for AI over the next several years[1].

1. *AI WILL DRIVE INFRASTRUCTURE DECISIONS*

The use of AI across enterprises is ramping up quickly. In fact, through 2023, AI will be one of the top workloads that drive infrastructure decisions. Accelerating AI adoption requires specific infrastructure resources that can grow and evolve alongside technology. AI models will need to be periodically refined by the enterprise IT team to ensure high success rates.

2. *MANAGE INCREASING COMPLEXITY OF AI TECHNIQUES THROUGH COLLABORATION*

One of the top technology challenges in leveraging AI techniques like machine learning (ML) or deep neural networks (DNN) in edge and IoT environments is the complexity of data and analytics. Traditional AI use cases that do not involve customer expectations are successful because of the tight collaboration between the business and IT functions, so securing the help of internal engineering teams is a must.

[1] *Predicts 2019: Artificial Intelligence Core Technologies, Gartner*

3. *SIMPLE MACHINE LEARNING TECHNIQUES SOMETIMES MAKE THE MOST SENSE*

Through 2022, over 75% of organizations will use DNNs for use cases that could be addressed using classical ML techniques. According to Chirag Dekate, Research Director at Gartner, "classical machine learning techniques are extremely underrated. Once you sift through the AI hype, you will realize that many organizations are pushing to apply deep learning techniques without even understanding how they apply to their current initiatives." As such, simplicity is key, and IT leaders should take the time to learn the spectrum of options to appropriately address their business problems.

4. *SERVERLESS COMPUTING WILL TAKE THE STAGE*

Containers and serverless computing will enable ML models to serve as independent functions and, in turn, run more cost-effectively with low overhead. A serverless programming model is particularly appealing in public cloud environments because of its quick scalability. Gartner says that IT leaders should identify existing ML projects that can benefit from these new computing capabilities.

5. *ADOPT AUTOMATION BEYOND THE SURFACE LEVEL*

As the amount of data that organizations have to manage increases, so too will the abundance of false alarms and ineffective problem prioritization. With the shortage of digital dexterity talent to effectively adopt AI, automation is a key solution.

"Although the potential for success is enormous, delivering business impact from AI initiatives takes much longer than anticipated", says Chirag Dekate. "IT leaders should plan early and use agile techniques to increase relevance and success rates". Therefore, to deliver successful AI initiatives, CIOs should:

- align infrastructure strategies with business use cases and requirements
- hire expertise in newer tools and techniques, or retrain existing teams
- standardize and broadly disseminate high-productivity techniques across the organization
- minimize time and cost overruns by using a combination of build, buy and outsource strategies, with mature tools and pre-integrated solutions

> “By 2023, 70 percent of AI workloads will use application containers or be built using a serverless programming model necessitating a DevOps culture.

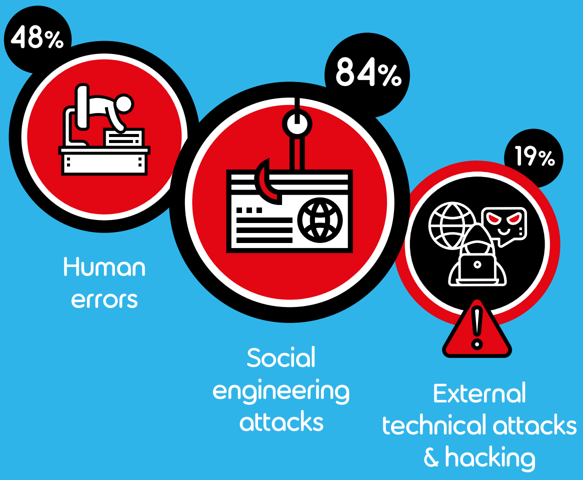
TELINDUS CYBERSECURITY REPORT 2019

Luxembourg-based companies reveal how they currently manage (or not) their cyber security incidents. Let's review the main pitfalls to avoid and the good practices you should implement to preserve your business!

The survival of a company in case of a security incident is inversely proportional to the time elapsing between the compromise & its detection and response. Efforts should be prioritised to increase readiness and response capabilities in conjunction with the increase of the detection capabilities.

Nowadays companies cannot manage incidents by themselves without information on the global current state of play. As a cybersecurity actor, we wanted to review the situation in Luxembourg. Cybersecurity incident management strategy shall no more be exclusively based on the prevention of recurring past known incidents. It is now mandatory to enhance detection, analysis and response capabilities by leveraging the strength of the community information sharing.

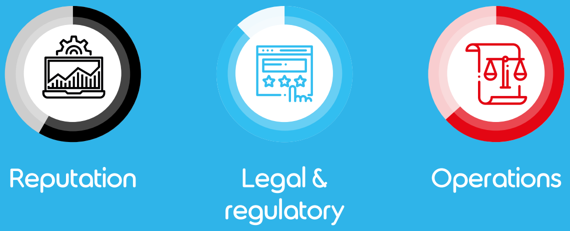
telindus



WHAT ARE THE MAIN CAUSES OF INCIDENTS?

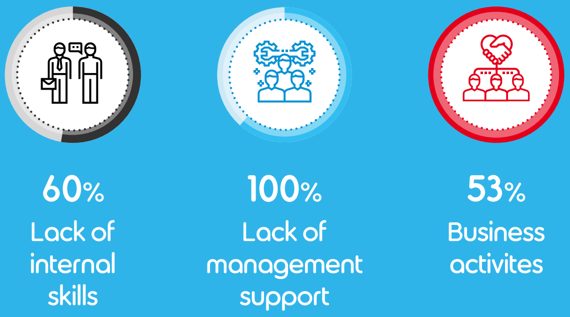
We, humans, are widely involved in security breaches and oddly, external threats and attacks are the far beyond our own mistakes when it comes to cybersecurity. Who would have thought so?

HOW DOES IT AFFECT YOUR BUSINESS?



You may think about financial costs first but... it's your reputation which suffers the most from a cyber-attack. Loss of revenue actually comes after your reputation, legal and regulatory. More surprising, 17% of respondents have absolutely no idea what financial impacts security breaches really have on their business.

WHY DON'T COMPANIES HAVE PROPER CYBERSECURITY SOLUTIONS?



Well, there is generally a cruel lack of support from the leading teams in cybersecurity matters. Internal lack of expertise has a role too, an efficient cybersecurity strategy requires strongs skills and experience. Half of the companies asked just focus on other activities and leave that crucial point... aside.

WANT TO KNOW MORE?

Download our infographics →

www.telindus.lu/en/cybersecurity-survey

Based on a survey conducted from May 5th to June 15th, 2019. Profile of respondents: CISO, ISO, IT Manager.

AI IN COMPANIES

THE CURRENT SITUATION

AN INVESTIGATION OF AI USE IN EUROPEAN AND BELGIAN MARKETS

Artificial Intelligence (AI) has been around for decades, but the rise in computing power promises whole new ways of using AI. Hence business is ripe with hype, and early adopters are spreading AI adoption from value chain to value chain, across all industry sectors. But what are these companies investing in exactly and how do they manage this complex transformation? Microsoft and EY investigated the currentstate of AI with European and Belux companies.

1. Current role of AI in business

HOW IMPORTANT IS AI?

Microsoft's report has shown that 90% of respondents in Belgium and Luxembourg say AI is considered an important topic with executives, but only 43% with managers and a mere 19% with employees. The reason might be that employees still share job insecurities about AI, and that AI is still very much an abstract notion to them. Not surprisingly, AI ranks high, but not highest, on the digital priority list. Priority is firstly given to collecting, storing and understanding data. Seventy-six percent of Belux companies have, however, initialized successful AI pilot projects or have started using AI applications in their daily operations.

WHERE IS AI CURRENTLY DEPLOYED?

Most AI in Belgium and Luxembourg is currently either deployed in IT (52%) or R&D (43%). Employees in R&D are often engineers with a proper understanding of and interest in AI. Very occasionally AI is also deployed in customer-facing and commercial functions like marketing, sales and customer service. But it is expected that these departments will make much more use of AI in the near future.

HOW IS AI PUT TO USE?

Firstly, 76% of respondents state that the main use of AI is to predict. For instance, AI can proactively and accurately predict which customers could leave. Secondly, 62% of respondents say AI is applied in smart automation mainly to automate logistics. The third main use for AI today is in

generating insights, which in Belgium and Luxembourg rates equally with automation at 62%. For example, AI significantly contributes to forecasting product demand. Finally, at 38%, AI is used to personalize the user experience, or to introduce chatbots to customer service.

2. Problems and advice from early adopters

The main problem that all companies share is a major lack of skilled workers to meet the demand for AI expertise. Hence many have either opted to seek external partners or they adopt a wait-and-see strategy. But pioneers advise not to rely upon external partners before having internal people who can properly evaluate their data. Also, adopting a wait-and-see strategy can prove risky, as the longer you wait, the harder it is to get the right people. If you do choose to form a relationship before you have in-house expertise, try academic partnerships, as they come with innovative and reliable ecosystems with a lot of potential.

THE PROBLEM WITH DATA

Another main problem facing companies is the governance of data, specifically who owns it, how it is stored, how it is accessed and who can access it. This includes external hurdles like privacy regulations (GDPR) and AI regulations, but also internal hurdles like organizational 'silo thinking'. Early adopters advise leaders to support collaboration through projects. Deconstruct decentralized data storage and introduce a centralized system where data is readily accessible. Cloud solutions can be a helpful tool here. Meanwhile the C-suite should focus on defining data governance and strategy, so that the company is not hindered by a lack of clarity. Finally, build your data structure to incorporate unstructured data, even from external sources.

NOT ENOUGH AGILE AI LEADERSHIP

The third most common problem is that AI leadership is lacking in the C-suite department. Leaders need to understand the impact AI has and needs to have on business. Change management should happen bottom-up. Leaders can support this by articulating a clear vision, by setting goals and securing a broad buy-in across the organization. In general, the company approach should be agile. So, break down silos and accept that leadership will lose control. Motivate exploration by starting experimental pilot projects and use cases with uncertain outcomes to learn where value is hiding and be prepared to adjust the company direction more frequently. The transformation is not immediate, it is continuous.

The benefits of AI

- 86% OF COMPANIES EXPECT AI TO OPTIMIZE OPERATIONS.
- 71% BELIEVE AI WILL TRANSFORM THEIR PRODUCTS AND SERVICES.
- 71% ARE CONVINCED THAT AI WILL AID IN ENGAGING CUSTOMERS.
- 62% SAY THAT AI WILL HELP EMPLOYEES IN THEIR DAILY WORK.

The risks of AI

- 52% OF THE SURVEYED ENTERPRISES ARE AFRAID OF AI'S IMPACT ON PERSONNEL.
- 43% SEE SIGNIFICANT RISK IN THE LACK OF CLEAR AI GUIDELINES AND REGULATIONS.
- 43% OF AI EXECUTIVES FEAR LOSING CONTROL OVER AI AND ALL THAT COMES WITH IT.

Read the full report on AI of Microsoft and get insights of several statistics.

→ ***PULSE.MICROSOFT.COM****/UPLOADS/ PROD/2018/10/WE_AI_REPORT_2018.PDF*

Source: *© **Ernst & Young LLP** in accordance with **Microsoft**, 2018*

CASE STUDY ESA*

PUSHING THE FRONTIERS OF CYBERSECURITY

*European Space Agency

Security of space systems and operations is essential for protecting critical infrastructure that affects every aspect of daily life. Communications, air transport, maritime, financial and business services, as well as weather monitoring and defense systems, would face serious disruption if satellites and space infrastructure were targeted in a cyber-attack. With the PenBox project, Telindus helps the European Space Agency (ESA) protect its assets and intellectual property, in particular through automating penetration tests and increasing user awareness. Marcus Wallum, Operations Data Systems Engineer at ESA, gives us some insights into the project and the issues at stake.

In a research paper published 3 years ago, The Chatham House – one of the most important think tank in international issues - raised the question of whether space was the final frontier for cybersecurity. The institute concluded its study by emphasizing that a radical review of cybersecurity in space was needed to avoid potentially catastrophic attacks.

HAS THE SITUATION EVOLVED SINCE THIS OBSERVATION, ACCORDING TO YOU?

M.W. If anything, the situation has become even more pronounced. Space systems and the data, products and services they provide are increasingly relied upon for supporting critical infrastructures and services, communication, scientific study, exploration, policy and decision making. This increased reliance of society on space assets also increases their attractiveness as targets for adversaries. At the same time, the number of governmental but also new private actors in the space domain are rapidly increasing as barriers to entry are lowered and new technologies enable more cost-effective access to space. As new actors enter the market and supporting infrastructure on ground becomes cheaper, more ubiquitously available and utilized, the potential attack surface and governance challenge increases, as well as the proportional cost of security compared to the cost of the mission itself.

At the same time, the extent and frequency of reported cyber security breaches and disclosures of critical vulnerabilities in widely used terrestrial software, hardware, platforms and systems is increasing. Together with the increasing complexity and tight coupling between space and terrestrial-based systems and emerging disruptive technologies such as hosted solutions which demand specific security treatments, it is apparent that the security of space systems, and a need to manage its effective application, has never been more important.

WHAT IS ESA'S PERCEPTION REGARDING THE DEGREE OF EXPOSURE OF THE SPACE INDUSTRY TO CYBER RISK?

M.W. Space systems and operations are almost entirely cyber-dependent, so of course there will always be exposure. More unique to the space industry are the security challenges that come with technology obsolescence, large and distributed supply chains, multidisciplinary engineering teams and the need to address security concerns beyond the controls and risk management approaches from well-known IT frameworks to account for particularities not covered by generic terrestrial systems.

> “ Telindus won the bid in open competition in which there were a number of strong competitors, which indicates the quality of their proposal.

WHAT POLICIES AND PRACTICES ARE IN PLACE IN THE AGENCY TO COPE WITH THE GROWING CYBER THREAT?

M.W. Today, cyber security is one of Europe's paramount concerns, which has triggered policy and institutional structuring efforts aimed at building a core cyber security culture and capability. At ESA for example, it will form one of the common underlying elements to the programmatic pillars presented at the upcoming ministerial council, emphasizing the need for a strong and comprehensive approach to cyber security and safety across all ESA programs.

ESA has a mature security governance framework with traceability from top-level regulations to directives to policies to implementation. This includes an accreditation and certification scheme, associated responsible roles and an ISO-27001 certified Information Security Management System.

Despite the increased focus, there is still much work to be done. For example raising sufficient awareness such that security requirements are supported from the start of a program or mission and flown down to the engineering level. The space system engineering lifecycle itself and associated standards require amendment to ensure that security is *baked* in by design. This is especially important as the complexity of systems continues to increase, demanding a need to fully understand any associated uncertainty. Emerging technologies such as AI, cloud infrastructure and digitalization similarly require thorough security analysis to avoid introducing uncertainty and vulnerability.

IS THE PENBOX PROJECT PART OF A SPECIFIC STRATEGY? WHAT ARE ITS MAJOR POINTS AND WHO IS IT INTENDED FOR?

M.W. The PenBox permits to execute generic penetration tests against a system in an easy and repeatable way for non-expert users, significantly lowering the cost and allowing repeatability of testing. Space mission-specific attack scenarios flag a potential real mission impact, greatly improving user and system-owner awareness. An easy-to-use user interface permits to visualize ongoing attacks and explore obtained results highlighting security requirement violations, discovered vulnerabilities and warnings. Report generation capabilities permit to capture detailed session results, for example for regression testing or security audits. Attack scenarios are configurable and adaptable to any kind of system and can be tailored to target only the desired systems. Security experts may fine-tune attacks, link new tools, etc. to improve the tests. There is still some work to do to fine-tune the executable scenarios and the requirements verification logic specific to the space ground segment environment – work now foreseen in a potential follow up project, however the proof of concept has been largely achieved.

Disruptive security and penetration testing are essential tools to integrate security into the ground segment system and software engineering lifecycle. An automated testing capability is therefore a key building block for the wider goal of achieving a DevSecOps type approach, where security is addressed continuously and throughout all stages of the lifecycle.

> “ The growing reliance of society on space assets increases their attractiveness as targets for adversaries.

Marcus Wallum,
Operations Data Systems Engineer at ESA

HOW IMPORTANT IS THE USER IN THE SECURITY CHAIN?

M.W. System security is only ever as strong as the weakest link in that system and, frequently, that link is the user. Raising awareness, also among developers, stakeholders and decision-makers is therefore key.

> “ An automated testing capability is a key building block for the wider goal of achieving a DevSecOps approach.

ARE YOU PLANNING TO ROLL OUT THE USE OF THE PENBOX TOOL TO OTHER ESA DEPARTMENTS OR TO INDUSTRIAL PARTNERS?

M.W. The PenBox was developed under ESA contract so there is flexibility in terms of distribution to interested parties. Strong interest in the tool has been expressed both by external industry and even other agencies, as well as by many departments of ESA, indicating the need for such a solution and justifying further investment in the future to improve on the prototype.

WHAT WERE THE REASONS PROMPTING ESA TO COLLABORATE WITH TELINDUS ON THIS PROJECT? WERE YOUR EXPECTATIONS MET? ARE YOU CONSIDERING COLLABORATING WITH TELINDUS ON OTHER PROJECTS?

> “ Raising awareness among developers, stakeholders and decision-makers is key.

> “ Strong interest in the PenBox has been expressed both by external industry and even other agencies.

M.W. Telindus won the bid in open competition in which there were a number of strong competitors, which indicates the quality of their proposal. Overall, the result is promising – some further work is required to realize realistic space ground segment-specific scenario execution and tailored attacks as well as reliable requirement verification logic. However, with the majority of the framework in place, this is not too far off and I am confident this could be achieved in any follow up activity. Having acquired yet more experience in ESA project work, Telindus continue to strengthen their position to compete for such future collaborations with ESA.

BLOCKCHAIN

SHAPING THE FUTURE OF TRUST

Frank Roessig, *Head of Digital Solutions for Finance at Telindus*

Blockchain is more than just a tool to enable digital currencies. At its most fundamental level, it is a new, decentralized and global computational infrastructure that could transform many existing processes in business, public administration and society in general. Blockchain has received considerable hype, ranging from "cryptomania" in the trading markets to widespread discussions about the breadth and depth of its potential impact across public and private sectors. We have asked Frank Roessig, Head Digital Solutions for Finance at Telindus, to help us gain a clearer understanding of the strengths of blockchain, as well as areas requiring improvement.

WHAT IS YOUR PERSONAL DEFINITION OF BLOCKCHAIN?

F.R. For me, in simple terms, blockchain would be a trusted and collaborative network for transactions and information. From a technical standpoint, it's a combination of three components. One of them is a chain of immutable blocks. The second component is a consensus mechanism, to get from n to n + 1, and the third aspect is a set of distributed ledgers. Combination means, for instance, that you may not have all three components but only two out of three.

WHAT ARE THE POSSIBLE APPLICATION FIELDS OF BLOCKCHAIN?

F.R. One application is, for example, notarization. Telindus has built the first European notarization log chain for the Luxembourg government. It is operational since 2018 and has been announced to the public and other European governments in February 2019. If you have a trusted source, instead of having to send back full force paper, you make a hash of a notarized document. You still have the notary that authenticates the document, but once he has evidenced it, he uploads a few hashes on the document and anybody who wants to compare a copy of the document just has to compare the hashes to check that it is verified. The advantage of that chain is that it significantly reduces the notarization log costs. It's a clear ROI.

Another application is traceability. We have built a traceability chain for any item in general but we have also built one version for IoT in particular. We are currently implementing such a chain with a company that produces very high-quality mechanical pieces. They want us to trace each piece from manufacturing via distribution to the utilization, the maintenance, and either the retirement or the breakage. That piece is used to transport expensive items and if it were to break, you need to know the history, for insurance purposes for example. These producers are being copied by cheap manufacturers and by using such a traceability chain, they can guarantee their clients that what they bought is actually an original, not a copy of any sort.

> “ Telindus has built the first European notarization log chain for the Luxembourg government.

Other use cases are what I would call KYX applications. There is a lot of KYX requirements and procedures - Know Your Customer, Know Your Supplier, Know Your Transactions, etc. Today all these KYs are done mostly bilaterally and repeatedly and for a lot of persons, the current KYX processes are highly redundant and inefficient, resulting in little added value. The idea is to put it on a chain once and then share it among all the parties who are entitled to see it. Once uploaded, it's verified, it's identified, because it's a trusted source. And then you decide if you want to share it with one or several of the counterparts, for example banks, you work with.

Telindus is working in a consortium with the Luxembourg Association of Corporate Treasurers, ATEL. Large corporates have joined us, including RTL, Koch, Aperam, Cargolux, Ferrero and Goodyear. They all have many banks they're working with and for every bank, they need to do their KYC. They wanted to work on a POC, where we upload the KYC once and then we share it with all the banks. We have talked to the ATEF and the ATEB, the French and the Belgian associations of treasurers, and together, we are exploring a cross-border framework for this."

Reconciliation is another application. Nowadays, reconciliation is done mostly bilaterally, especially in the fund industry, between the various members of the fund administration value chain. As a result, mismatches tend to be modified only between two entities. Blockchain-based reconciliation works among multiple parties, live, in parallel, and transparently on chain.

Blockchain may also complement AI and solve the problem of trust many people face with this technology. One of the challenges with AI is the veracity of the underlying information. If you start blockchainizing the information you feed into AI, you can enhance the source and the whole history of what the AI is using. That's a potentially explosive use case that might permit far better and more concrete applications of AI.

> “ Blockchain may complement AI and solve the problem of the veracity of the underlying information.

There is also a key application that I call interchainability. The reason is that we're all not going to use the same chain. It is like with operating systems: I mean we have Linux, Apple, Microsoft, etc. It's going to be the same on blockchain. Actually, there's going to be a whole conundrum of blockchains and it is therefore essential that chains communicate with each other in order to scale and enable more use-cases...

We are also talking to a few big corporates with over 300 intra-group entities. That's another use case. They do interco financing and interco-payments, and they have no view of what is really happening. They want to put it on a chain and see how it can improve their monitoring as well as their cash management.

Another use-case is the optimization of transactions: payments, trade finance, capital market securities. All these are the biggest use cases: notarization, traceability, KYX, reconciliation, interchainability, and transactions in general.

WHERE DO WE STAND IN LUXEMBOURG? WHAT ARE THE MAIN OPPORTUNITIES FOR OUR BUSINESSES AND ORGANIZATIONS?

F.R. I would say that in Luxembourg we actually passed the hype cycle and we are entering the application world. We can clearly feel that people are now in a mindset where they would like to get things going. It is true that we have a few consortiums that have failed. But I think that most of them failed because the use cases have not been described or defined properly and also because they didn't work in an agile manner.

I believe that to make things work with a new technology, you need two things. First, you need to have a clear ROI, a return on investment that you must be able to define with all the stakeholders. Secondly, you must be able to start in a lean manner with low budgets.

> “ The whole ecosystem in Luxembourg is definitely in action mode.

As I said in my prior example, Luxembourg has the first notarization chain in Europe and that way, the Luxembourg government has also proven that they favor innovation, that the whole ecosystem in Luxembourg is definitely in action mode. The government has also announced that they wanted to create a government blockchain. The use cases are not clear yet but they have a few ministries involved, along with SIGI - the Syndicat Intercommunal de Gestion Informatique - and the idea is again to see what can be blockchainized in an efficient manner on the government side.

> “ Blockchain is clearly a source for faster, cheaper and more secure transactions.

WHERE IS, IN YOUR OPINION, THE GREATEST POTENTIAL OF BLOCKCHAIN TECHNOLOGY?

F.R. I would say that one is a disintermediated and trusted interaction between parties. So, if I know that somebody uploaded an information on a chain and that I can trust it, I don't need somebody centrally located to tell me again that this is a source of truth. The system has validated it. And we can for example exchange between ourselves something like a payment without having a central guarantor.

We talked about transactions earlier on. Blockchain is clearly a source of doing transactions that are faster, since there is no need to have a T+2 any more in the financial world. But it could be more than just payments. It could be transactions for assets of any sorts or even for trade finance export documents or whatever else. It should be secure because blockchain has this immutability that makes it impossible for anybody to tamper with the system. And the third thing is that it should be cheaper. Today, a SWIFT transaction costs around 50 dollars. The same type of payment using a Stellar blockchain for example costs less than 0.5 dollar. So, clearly, those transactions should become much cheaper.

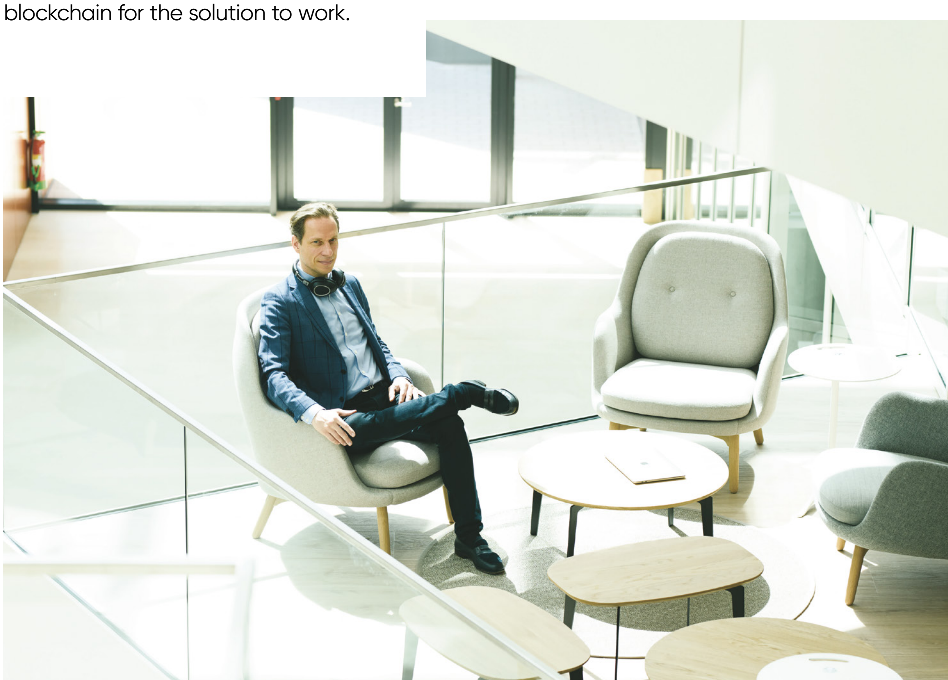
The third aspect is what I call a distributed source of truth in general. Any time you want to validate something - Is this a real picture? Is this the hotel payment I made? - you don't need to go to a central source. These are the three main potential development areas: disintermediated interaction, distributed source of truth, and faster, cheaper and more secure transactions.

HOW DIFFICULT IS IT TO GET STARTED WITH BLOCKCHAIN TRANSACTIONS? SHOULD THERE NOT BE AN INTENSIVE AND THOROUGH DIALOGUE BETWEEN THE STAKEHOLDERS, WHO DO NOT NECESSARILY HAVE THE SAME DEGREE OF MATURITY IN THIS MATTER?

F.R. I would say first that we built an interesting module at Telindus. It's called Blockchain as a Service. It's an interface where you don't need to know anything about blockchain at all. You can start creating a node and create a smart contract very simply. It will not produce a full solution but if you have never heard of blockchain, you can start playing around and actually see what it can do. This kind of environment makes it much easier for people to start to experiment with blockchain and see what it does."

If you look at a blockchain solution, blockchain itself accounts probably for between 20 and 30 percent of the solution. All the rest are interfaces, back-ends, data management that you must agglomerate around the blockchain for the solution to work. For a lot of users, they don't even need to know it's a blockchain they are working with. They certainly will work with something that is much faster, much cheaper, and much more efficient. The knowledge can be limited to the people who build the chain and the interfaces, which leads me to the second point of the question, which is stakeholders. And that is really key.

> “ That's what we are building for people: We make blockchain as easy as a click on a button.



You need to integrate the stakeholders from scratch because a blockchain for its own sake doesn't help anybody. You need to get everybody around the table and present them the advantages that you want to get out of this chain. And you need to engage in this very early to reassure them saying 'No, you do not need to learn about crypto currencies or build the wallet', because that's what they read in the press. Today, when you want to create an account on blockchain, you either have to go to an exchange with a simplified version or else you have to create a wallet, have your private address, your public address, to start playing around. What we actually do at Telindus is we will build the whole layers on top of this, the back-end, the chain, the smart contracts, the front-end that will make you use the chain without having to know anything about what a chain is. And that, in my mind, is the future of blockchain.

If you go on the web today, you use a browser and you do whatever you do. You don't have to go back and type the HTML code yourself, like the first internet users did in the 90s. At that time, when you were going online, you still had to type every address by hand. Today, you just click on a button. That's what we are building for people: they just have to click on a button and start using blockchain. My intimate conviction is that, in the future, it's going to be as easy as talking to a machine.

ACCORDING TO THE WORLD ECONOMIC FORUM (WEF), BLOCKCHAIN COULD ACCOUNT FOR AS MUCH AS 10% OF GLOBAL GDP BY 2025. ON THE OTHER HAND, WEF EXPERTS ALSO UNDERLINE THAT REALIZING BLOCKCHAIN'S POTENTIAL WILL REQUIRE FIXING CURRENT TECHNICAL LIMITATIONS AND ADDRESSING REGULATORY AND LEGAL CHALLENGES. WHAT IS YOUR PERSPECTIVE ON THESE ISSUES?

F.R. We, at Telindus, are part of the ALCO Crypto-Asset Working Group. And as a working group, we have produced a white paper on how to do compliance on these new types of assets. We are really involved in this and we are aware that it raises a lot of interest and passion. In fact, there are two angles to this. On one side, the blockchain technology will have to adapt to the existing regulation. If I look at KYC, KYC regulation is not going to be changed because suddenly there is a blockchain. You still need to make sure that you know who the customer is. So, the technology must adapt in a certain manner to the regulation. But it is true that, to a certain extent, the regulation must also adapt to the technology. Let me take the example of GDPR and the capacity to destroy your data. There is a way to destroy or make the data inaccessible on a chain. What does that actually mean if you say 'the data is going to be destructed'? Because, even if you erase a hard disk, we all know that some police forensics experts can look at it and find something. It's the same on blockchain: you need to ensure that the data is actually not accessible anymore. There, I think that the chain has to adapt to the regulation, there's no question.

> “ The regulation and the blockchain technology need to adapt to each other.

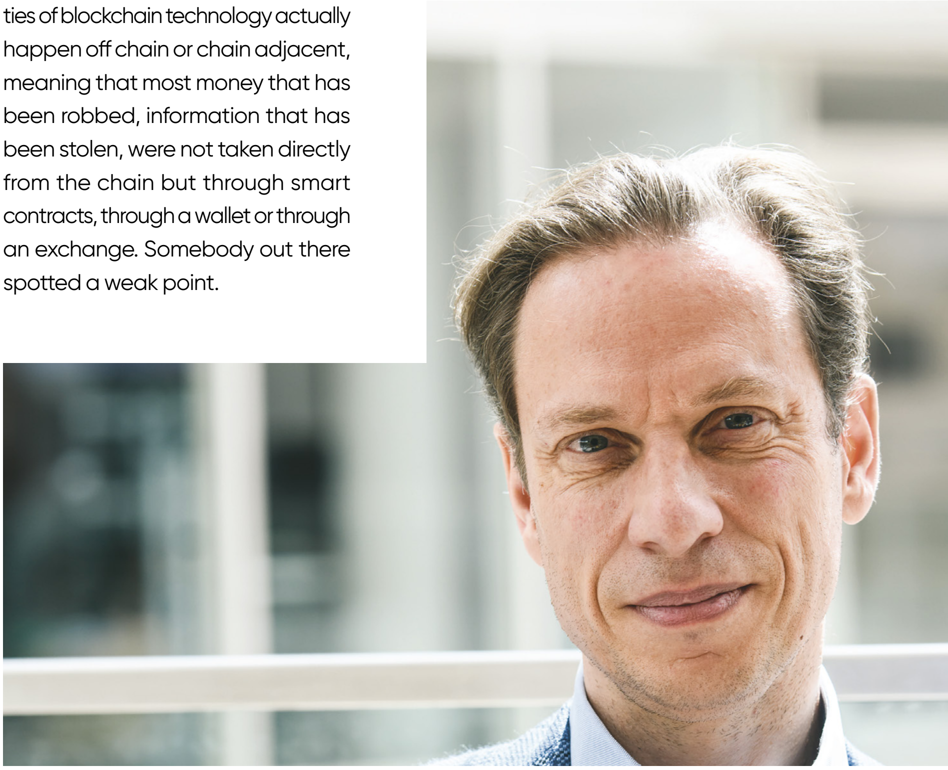
Now, sometimes the regulation needs to adapt to blockchain technology because there is simply no way to do otherwise. You cannot totally tweak technology. For example, if you have public and private addresses on blockchain that are being used to do transactions, when you are doing KYT – Know Your Transaction - on blockchain, you will not trace the name of a person, you start tracing addresses. And by tracing addresses, then you can trace more or less the legality of a transaction. There, the regulation should consider tracing addresses instead of people's names because addresses are the only things available at a certain stage.

AML 5 is another interesting example. The 5th Anti-Money Laundering Directive has created a set of rules around blockchain that are especially aimed at exchanges. Exchanges must report on any transaction between fiat currencies and blockchain. They must do the same KYC, the same transactions. But at this stage, they have not included transactions between chains. Let me take another example. If Facebook Libra takes off, it's a huge game changer in how people are going to do payments, based on a chain. But it's also about interchainability, meaning that people do payments between chains. I will use my Libra and convert it to use Lumens for example. Here again, the regulators should address the issue and also monitor the transactions between the chains. Because the technological possibility exists and will not disappear.

> “ We need to work with trusted people. This is why we are part of the Infrachain initiative.

BLOCKCHAIN HAS A REPUTATION FOR BEING FRAUD-PROOF, WHICH CONTRIBUTES CONSIDERABLY TO ITS ATTRACTIVENESS. BUT WITH NEW TECHNOLOGIES SUCH AS AI AND AUTOMATION GAINING MOMENTUM, THE POTENTIAL RISKS OF CYBER-ATTACKS ARE ON THE RISE AS WELL. WHAT ARE THE POINTS OF VULNERABILITY OF THE BLOCKCHAIN TECHNOLOGY?

F.R. Per experience, most vulnerabilities of blockchain technology actually happen off chain or chain adjacent, meaning that most money that has been robbed, information that has been stolen, were not taken directly from the chain but through smart contracts, through a wallet or through an exchange. Somebody out there spotted a weak point.



I think the biggest case is the Ethereum one, where users exploited a vulnerability in The DAO code to enable them to siphon off one-third of The DAO's funds to a subsidiary account. They stole the Ethers from their organization but the rest of the chain remained untouched. That's a very important point because, if we think about it, one of the oldest chain is Bitcoin. And if you actually managed to attack it, you would get over 100 billion $ in value. And I think that a lot of hackers would like that. But so far it has not happened. If it was possible to hack the chain directly, we would know by this time. That's where the main vulnerabilities are.

It also means that you need to work with trusted people. It's also an occasion to talk about an initiative we are part of. It's called Infrachain and was kicked off by Telindus and other actors of Luxembourg's blockchain industry in order to create industry-scale resilient blockchain nodes. At this scale, you need nodes that are totally secure and also that are always operational so as to ensure the continuity of transactions. Because losses may be due to the theft of information as well as the disruption of transactions. That's a huge issue if you are in the financial industry. Initiatives like Infrachain identify and pre-emptively counter potential future threats.

CAN WE CONSIDER THAT, LIKE THE EARLY INTERNET, BLOCKCHAIN MARKS THE BEGINNING OF A NEW TRANSACTIONAL PLATFORM?

F.R. Blockchain is a game changer in terms of technologies and new business models. I strongly believe that it beholds business models for enablers. And in fact, I would describe it a bit more in terms of platform, as, in my mind, we're entering the post-platform era. It's more like the Internet. The new Internet of truth and the Internet of values. And actually, it's a network of networks. So, the platform provider will gradually disappear to be simply substituted by trusted network providers.

I think blockchain will pressure the platform economy to evolve into what I would call the pure network economy. It means that the provider of the network will enable you and then you will lose exclusive control of it nearly immediately. It's not going to be yours anymore and become, like the others, a participant, a founding participant.

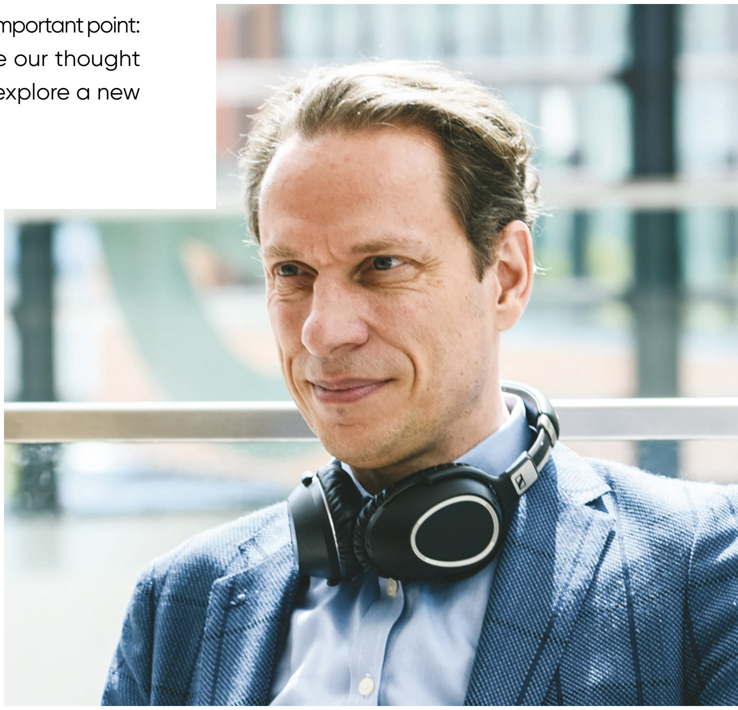
As a network enabler, an actor like Telindus would play a key role. On one side, we will make sure that we provide the nodes but also allow people to operate on the network, we will provide the access to build the applications that will work on it. But we're not going to control the network anymore, that's going to be beyond our control. People would come to us and say "look that's what I want to do in this network". And we'll say "OK, we'll build that solution, that's going to work on the network". So, people are going to come to you, having their requirements, and you just provide them with a solution so they can operate on the network or with a technology with their nodes on the network. I think that's it: from platform to network economy.

That's really important. It goes back to interchainability, so being able to be a provider of interoperable solutions because the other person on the network may use a totally different protocol. But still we need to talk to each other, which is why we need to build bridges to interact with each other.

> “ With blockchain, we are about to shift from a platform economy to a network economy

Blockchain will be the source of trust, truth, and fast, secure and cheap transactions for this network economy. We don't know what the business models are going to be but we really need to be prepared like to say "OK, I'll give you this component". And that's it, you take it and run with it. I mean if the corporate uploads information on that chain, you give them the chain, you can even operate the Chain as a Service, but then you're basically done. Having said so, it's going to obviously raise questions of governance. Being a member of the W3C, I have seen that these questions are often discussed and in continuous evolution.

But they're going to be essential because technology is also going to require governance to enable change. That's a very important point: We need to change our thought patterns in view to explore a new future...



EMERGING TECHNOLOGIES

BOTH THREATS & ANTIDOTES

Ralf Hustadt,
HPC & Big Data Lead at Telindus

Cédric Mauny,
Cybersecurity Lead at Telindus

Big Data and AI technologies are certainly the driving force behind a variety of technological innovations, from personal assistants through chatbots, autonomous machines, self-driving cars, and unmanned aircraft systems to natural language interaction. With all the benefits, however, come substantial risks. We have asked Cédric Mauny, Cybersecurity Lead, and Ralf Hustadt, HPC and Big Data Lead at Telindus, to share their insights and explore the implications.

BIG DATA PRESENTS A GREAT OPPORTUNITY NOT ONLY FOR BUSINESSES BUT FOR CYBER CRIMINALS: THE BIGGER THE DATA, THE HIGHER THE REWARD FOR THE MALICIOUS INTRUDERS. WHAT ARE THE MAIN SECURITY CHALLENGES FOR BUSINESSES AND ORGANIZATIONS AS REGARDS BIG DATA?

RH. "One of the main threats posed by emerging technologies is the fact that most of this is fairly new and is developed in a very agile way. Assuming you are coming from the academic field with a state of the art technology in AI that you want to sell, you'll be focusing on solving the problem, while the surrounding environment is not your top priority. One of the key aspects they typically doesn't get consideration from day one on, is how to make the system itself secure. The aim is to develop an algorithm or a system that works and solves a given problem. That does not necessarily mean that it is safe per default. We have also seen that when it came to high-performance computing especially with platforms hosted in the academic world, for example. If you look at it, why do large corporates operate their own high-performance computing platforms? Simply because they would never entrust confidential data to a university where a student can more or less walk in with a USB stick. That counts for physical security, for access rights, and all the other security-related topics."

CM. "That also counts for privacy. Big Data is a consolidation of lots of different data and this creates new risks for personal data, because inferences could be derived from such large volumes of data, for instance."

RH. "Let me give you an example to illustrate this. Let's say you found a way to gather a lot of data and you have developed a new algorithm or process to do something with it. You create a system, set it up, give access to the different customers and then you find out that there is no clear separation for the access rights. So, you end up with a system where someone, with a little bit of knowledge and malice, can access somebody else's data."

"The key thing here is not that this done on purpose. It's simply that a Data scientist is not a security or compliance expert and might not aware of these issues. The same counts for the code. If you code something and create a system that works, maybe you forgot to change the default passwords, failed to use secure coding techniques, or have not put the right protection mechanisms in place. All of this constitutes a major security challenge in a Big Data environment."

AND WHAT ABOUT ARTIFICIAL INTELLIGENCE? LET'S IMAGINE THAT CRIMINALS, ROGUE STATE AGENTS, UNSCRUPULOUS COMPETITORS, OR BLACKMAILED INSIDERS DECIDE TO MANIPULATE AN ORGANIZATION'S AI SYSTEMS, FOR EXAMPLE. ANOTHER CONCERN IS THE POSSIBILITY THAT ATTACKERS USE AI IN A VARIETY OF WAYS TO EXPLOIT VULNERABILITIES IN THEIR VICTIMS' DEFENSES.

CM. "Today, Artificial Intelligence is used to strengthen security, but it is also utilized by attackers and this is something that we can't ignore. Our view is that AI, by accelerating the processing of massive volumes of data, will help detect attack patterns. The whole security community is counting on that trend continuing and improving. However, we must not forget that attackers actually use the same technologies - and sometimes even better than us - to carry out their criminal activities."

RH. "I'll give you a very simple example that is not exactly related to using AI, it is rather a case of subverting AI. Large companies today use AI for filtering CVs. The HR department puts the CV in pdf format into the machine and the machine selects the resumes of the candidates to be interviewed. What do you do if you know that they are using such a system? And how do you actually bypass the system? It's quite simple. If you have some keywords in your CV that signal a certain expertise or a high potential, the likelihood that you will be selected for an interview is much higher. Of course, you cannot simply lie on your CV pretending that you hold a PHD from Harvard. Since a human reader is expecting black characters on white paper and a machine cannot distinguish between the real text and the subtitles, you can simply type PHD Harvard in white characters on white paper in a subtitle. So, your keywords are not visible to a human reader and, as the machine doesn't always give the reasons for its choice, your chances of being screened in are increased."

CM. "In this particular case, you can mislead the AI because the selection process is only based on keywords. But special security measures are probably foreseen to address such situations, such as submitting the outcomes produced by the algorithm to a human verification. It is important to keep in mind that automated individual decision-making, in other words deciding by automated means without any human involvement, is framed by the GDPR."

> “ Today, Artificial Intelligence is used to strengthen security, but it is also utilized by attackers and this is something that we can't ignore
>
> **Cédric Mauny, Cybersecurity Lead at Telindus**

"There are also some ways for manipulating supervised Machine Learning. Some consist in forcing the machine to learn by behavior and to consider a bad behavior as the normal baseline. Consequently, upcoming attacks may not be detected because being identified as falling within the scope of normal behaviors."

YES, BUT WE CAN PRESUME THAT THIS IS UNLIKELY TO HAPPEN. DON'T YOU NEED AN INSIDE MAN TO PULL OFF SUCH A FRAUD?

"In fact, you don't know the status of your information system when you set up such a Machine Learning process. Therefore, you assume that your information system is secure and trust it. But what about if an attacker is already in place? There is no silver bullet solution to secure such a system. You must rely on composite measures made of usual behavior, rule-based analysis, pattern matching, variance from a company standard, etc."

IN THIS REGARD, BIG DATA ANALYTICS SOLUTIONS, BACKED BY ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING, GIVE HOPE THAT BUSINESSES AND PROCESSES CAN BE KEPT SECURE IN THE FACE OF A CYBERSECURITY BREACH AND HACKING. HOW CAN THESE TECHNOLOGIES BE USED TO IMPROVE DATA PROTECTION TECHNIQUES AND CYBER THREAT DETECTION MECHANISMS?

RH. "Typically, cybersecurity solutions today are, to a greater or lesser extent, built around a system that triggers an alarm if something unusual happens. And it's up to you to define what something unusual actually is. If it is trying to access the network from the outside, you can easily define that. But what does unusual mean in terms of user behavior?"

"If your company is a big consulting firm, users are probably behaving differently than in a company like ours, for example. The profile of a consulting firm is probably different from that of an ICT company where we more or less stick to regular working times. For a consulting firm, on the other hand, it's seems completely normal that people access files in the middle of the night, due to the fact that they are working in a global organization with different time zones, or because they are in a rush to complete an important project."

"So, how do you define what an unusual behavior is? You could probably discover it but you simply don't have the time to explore all these amounts of data. An unusual behavior could be an employee who is accessing specific folders at odd hours and is trying to copy the content of those files, or who is attempting to delete them. It seems legitimate to have a short conversation with this employee to clarify this issue. But you can't, because of a lack of time and resources. The big advantage of AI is that it enables you to define a normal status and let the machine watch for deviations from expected behavior, twenty-four hours a day and seven days a week."

CM. "I believe that AI, Machine Learning, and other emerging technologies could be used to bridge the skills gap and to allow humans to focus on the most important information. AI systems, for instance, are able to process large volumes of data and extract trends from this data, or to highlight specific aspects to focus on. Inversely, human beings are able to take decisions on the basis of small quantities of data, which is very difficult for AI. To put it simply, Artificial Intelligence is highly relevant at the very beginning of the process, when extensive sets of data are involved while humans can focus on small sets of data. This is precisely the way we proceed at Telindus' CyberSecurity Intelligence and Operations Center (CSIOC) e.g. our SOC."

"One of the outcomes of this approach is a set of tools called SOAR - Security Orchestration, Automation and Response. SOAR is a software stack that allows an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance."

RH. "Typically, humans can naturally perceive if something is not normal. A standard system cannot do that. Therefore, you have to teach an AI everything by rules, whereas man uses his brain. For example, if a computer in your system is accessing a file server, it's a standard normal behavior. If the computer in question suddenly starts addressing all systems in the middle of the night, it's definitely not normal. But unless you have told your surveillance system to look for that specific behavior, it won't recognize it."

"One of the SOAR platforms mentioned by Cedric is Splunk Phantom. We have a sister company in the Netherlands, Umbrio. Among other things, this solution is capable of going through large data files on a flow basis, in near real time. That's the key asset of that system, because it doesn't really help if you collect data but you need three days to discover that somebody breached your system ... three days earlier."

CM. "The same approach applies to Security Operations Centers. Our CSIOC, for instance, relies on different sets of detection rules: based on known patterns - someone establishing connections on his laptop in the middle of the night - on data volume, on variance compared with average values, on AI-based pattern detection, and of course on human analysis."

"AI is a very useful tool for processing large data volumes and detecting patterns, but in the end, we rely on human experts. This also counts for our penetration testing projects, for which we use AI-based tools to perform the first level of analysis. After that, as a second step, a human consultant, backed by his experience and knowledge, takes over and makes the decision to dig to go further in one direction or another. We recently conducted an automated penetration testing project for the European Space Agency that illustrates this point[1]."

"It's important to understand that these emerging technologies are utilized by both defenders and attackers. Attackers know that defenders are working with AI-based tools. But we have to keep in mind that they are using the same means. We need to know our enemy so as to fight him with the best weapons."

RH. "I think that the big challenge with AI-based automated threat detection solutions is that you need to teach the system. And in order to teach it, you need to have, let's say, good and bad examples. It's not enough to tell the system what the normal state is. You also have to show the system what an attack does look like. You need to have both data sets."

"Let me use a simple metaphor. If you want to teach a system what a cow looks like, you need pictures of cows but you also need pictures of other animals, or else you won't be able to tell your system what the difference is. Having only data on your network

[1] *See "Pushing the Frontiers of Cybersecurity" p30*

when it is not under attack is similar to trying to find a cow in a herd of animals without knowing what other animals look like. It is hard to teach a system what an attack looks like if you cannot show any examples. That's currently the main challenge that we are facing."

CM. "It's a paradox. We need to teach AI good and bad examples, but for that we must decide what good and bad examples are. And we could end up with a situation where we would need another AI to teach the AI good and bad examples."

RH. "We are facing the same issues in the financial sector. You cannot teach the system to detect fraudulent transactions if you only have patterns of regular behaviors. And moreover, these behaviors are likely to adapt and change over time."

CM. "If a given behavior changes, it is difficult for us to detect the new behavior. Let's take an ICT company running a new service as an example. A new service triggers new connections, which represents a huge variance from the data of the day before that can be understood as an abnormal event by the surveillance system. This is why it is very important to keep on learning. And continuous learning means sorting between good and bad examples. At the end, this is a question of data quantity vs data quality."

SO, THIS UNDERLINES THE IMPORTANCE OF THE ROLE PLAYED BY HUMAN ACTORS?

RH. "Yes, the machine is always a support. The only situation where a machine is much better than a human being is in processing massive data sets. And since it can be trained to recognize the knowns, AI is perfectly geared towards an initial triage."

AND WHAT ABOUT PRIVACY AND PERSONAL DATA PROTECTION?

CM. "I believe that Big Data may raise privacy issues that we don't know yet. For the time being, we do not have any idea of what will raise from the aggregation of those tremendous amounts of data. Just think of China's rapidly expanding networks of surveillance cameras. We also leave many traces behind us on the internet that may raise serious issues if they are correlated with one another. Take the Cambridge Analytica scandal, for example."

RH. "I think that the best protection in this case is knowledge and awareness. There are a lot of cases where people are not aware of these issues. For instance, as a customer, you may be involved in one or several loyalty programs. A loyalty program is an agreement between a business and its customers where customers agree to allow the business to track purchases and in return, the business offers rewards such as coupons, cashback, lower prices or a free product or service. Today we have moved from simple paper punch cards to electronic scannable cards and smartphone applications. These programs are important for marketers and data miners, because they allow the business to track the customer's purchasing behavior in detail."

> “ Humans can naturally perceive if something is not normal. A standard system cannot do that. Therefore, you have to teach an AI everything by rules, whereas man uses his brain
>
> **Ralf Hustadt, HPC & Big Data Lead at Telindus**

"Some uses of your shopping information can seem safe enough: you give those businesses access to what you buy, and they give you discounts or freebies for spending money with them. But what is not immediately apparent is the hidden cost. When you enroll for the loyalty program of your favorite store, you may also agree, more or less voluntarily, to enroll in a targeted advertising program that shares your personal details and buying habits with other companies, who can then use them to target you as a potential customer. And on top of that, those companies can also enrich the data they have collected about you by buying customer data from third-party companies, known as data brokers."

CM. "It's a matter of balance between usability and privacy. And I think that we are well advanced in this regard. I have heard that retail platforms had obtained a patent for shipping products to consumers with autonomous flying delivery drones before they even order them. The technology or process to deploy is called anticipatory shipping. This is the next step of the optimization of the supply-chain: to cut down on processing and delivery times, the items will not be sent from a central warehouse directly to customers, but rather to a nearby shipment hub. The anticipatory shipping process will leverage predictive analytics tools along with the massive volume of customer data accumulated during previous orders, basket or shopping cart contents, or wish-lists."

"There is one more thing that people are not aware of. Did you know that, even if you didn't have a Facebook account, Facebook had probably created one on your behalf, a shadow profile, based on the data that the social network collects from other users? The term shadow profile refers to all information that you have not communicated to Facebook but it still has on you, whether you have an account or not. These shadow profiles are mainly fed by information from your friends, be they online or in real life. It is enough that one of your contacts has shared his phone contacts with Facebook, or his email address book, or that he has mentioned information about you on Messenger, for Facebook to gather and keep them in a kind of virtual file about you. This practice clearly raises questions around data collection, consent, and personal data protection."

RH. "The nice thing is that you can also use it the other way round. It has been done before by the police forces in the U.S. who had identified a network of criminals but didn't know who was pulling the strings in the shadows. So, they analyzed the criminals' Facebook accounts and found that there were almost no relationships between them but that they all had connections with one particular individual who turned out to be the godfather of the organization."

CM. "To conclude, I would like to underline some important points. AI, Big Data and emerging technologies are the future, not only for enterprises, but for all humankind. They come with enormous opportunities, but also threats that are difficult to predict. The reality is that any innovation might be used for both beneficial and harmful purposes. The development of such technologies needs to be audited, mapped, governed and prevented when necessary."

Augmented Intelligence, a Human-Centered Partnership Model

By combining the strengths of artificial and human intelligences, Augmented Intelligence, also known as AI Augmentation or Decision Support, is changing the game for cybersecurity, helping to analyze massive quantities of risk data to speed response times and augment under-resourced security operations.

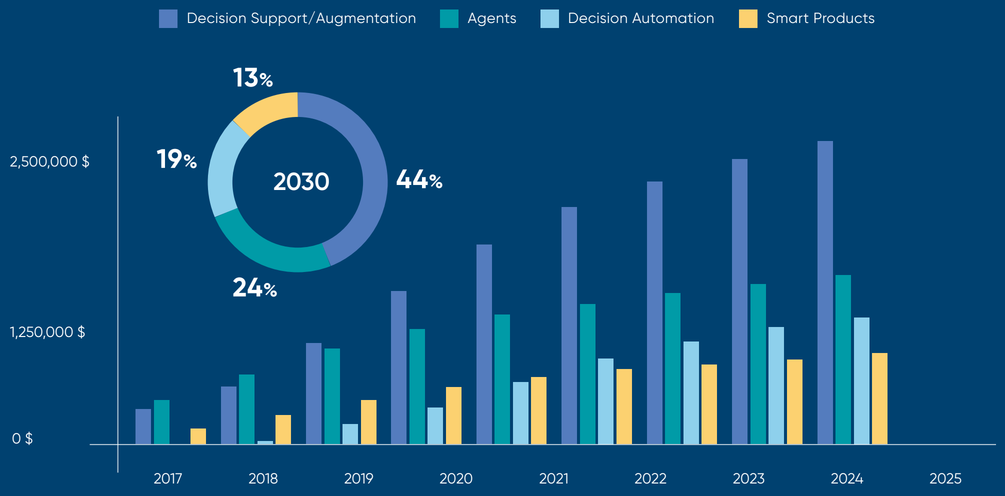
A new research provided by Gartner[1] suggests that humans and AI working together to enhance cognitive performance is set to become the most valuable application of AI technology, at least in the near future. In 2021, AI augmentation is set to create $2.9 trillion of business value and 6.2 billion hours of worker productivity, globally.

Gartner defines Augmented Intelligence as a human-centered partnership model of people and AI working together to enhance cognitive performance. This includes learning, decision making and new experiences.

In 2017 and 2018, AI augmentation was second among AI technologies in terms of the value that it creates for businesses. Gartner predicts that it will rank first this year and then explode as we reach 2025 becoming about twice as valuable as the AI technology in second place, virtual agents.

According to Svetlana Sicular, research vice president at Gartner, "Augmented Intelligence is all about people taking advantage of AI. As AI technology evolves, the combined human and AI capabilities that augmented intelligence allows will deliver the greatest benefits to enterprises. The goal is to be more efficient with automation, while complementing it with a human touch and common sense to manage the risks of decision automation."

Business Value Forecast by AI Type



Source: © Gartner

[1] *Gartner, "Leverage Augmented Intelligence to Win With AI", August 2019*

GETTING AI INTO WORK

HERE & NOW

Many organizations are confused about how to adopt emerging technologies easily and cost-effectively. With Artificial Intelligence and Machine Learning on everyone's minds these days, the constant threat of disruption from the next big thing can be paralyzing. For Emma Hitzke, Senior Director, Emerging Technologies, Oracle, AI and ML have already much to offer those who embrace them, provided that certain important principles are observed.

ORACLE

HOW CAN ARTIFICIAL INTELLIGENCE HELP IMPROVE THE EFFICIENCY OF BUSINESS FUNCTIONS?

E.H. Like any technology, AI and ML are tools that can solve a business problem. By starting with your business needs instead of focusing on the technology, you put the business value at the center of your transformation efforts. For example, if you are a CFO looking for ways to automate repetitive processes such as cash disbursement and revenue management, or to close the books more quickly, efficiently, and accurately, then an ERP solution with embedded ML can deliver on these promises. Actually, a research from the McKinsey Global Institute found that 40% of finance activities can be fully automated, and another 17% can be mostly automated. The bottom line is that AI can improve automation, predictions, and decision-making while lowering costs and improving efficiency.

When coupled with analytics, AI can provide unprecedented capabilities to better manage the business, make decisions, and discover patterns. AI can improve business functions in three primary ways. First, by improving productivity, efficiency, and engagement. Next-gen experiences such as conversational interfaces and intelligent user experiences can simplify multiple tasks. Secondly, AI allows for tasks automation, which not only reduces costs and improves accuracy, but also liberates people from performing mundane work and allows them to focus on more strategic projects. And finally, Machine Learning can help improve predictions and increase the accuracy of forecasting or budgeting which, in turn, supports more informed decision-making.

> “Advanced technologies require a receptive culture and the ability to provide highly relevant data for analysis

WHAT ARE THE CHALLENGES AND REQUIREMENTS FOR SUCCESSFULLY IMPLEMENTING EMERGING TECHNOLOGIES SUCH AS AI?

E.H. Advanced technologies cannot bring about transformation on their own. They require a receptive culture and the ability to provide highly relevant data for analysis.

You must first consider the cultural shift that new technology creates. Improving communication is a major component of a successful AI initiative. If your business and IT teams are not communicating already, adding AI won't improve the situation. The process begins with aligning one another's expectations, which means sharing business objectives and clarifying the scope and timeline of any new initiative.

You also need to bear in mind that even the best algorithm cannot provide meaningful insight if the data you start with is not of the highest quality and relevance. You need to have data-cleansing processes such as de-duplication, and plan to augment data you have collected with additional information derived from internal and external sources, combining internal financial data with internal HR data or external business bulletins, for example. Most importantly, you must liberate your data from functional and operational silos across the organization.

Another challenge is to address security concerns. The explosion of data held in corporate systems is already raising red flags around security and privacy issues. Organizations must learn how to maintain the security - not to mention anonymity - of the data they collect and process in order to retain customer trust and comply with regulations.

Lastly, but certainly not least, acquiring new skills is an essential step in the process of implementing data-intensive technologies. The drive to mine data for insight has made data scientists a hot commodity. Once your business teams acquire the skills required to extract meaning from your data, they will be able to derive the full benefit of AI.

> “40% of finance activities can be fully automated, and 17% can be mostly automated
>
> **McKinsey Global Institute**

TO BE MORE CONCRETE, HOW CAN ORGANIZATIONS TAKE ADVANTAGE OF AI TO IMPROVE THEIR DAILY ACTIVITIES?

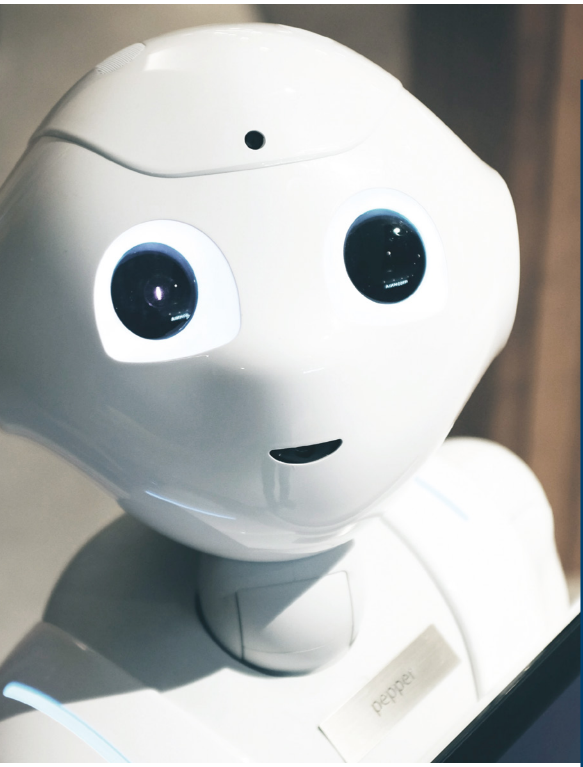
E.H. When software solutions come with AI already built in, organizations can embrace the latest innovations right away to improve user engagement, collaboration, and performance. Applications such as Oracle ERP Cloud include ML capabilities embedded within familiar user interfaces and business workflows. They enable enterprises to realize quick value from the latest innovations in AI, conversational interfaces, natural language processing, blockchain, and the Internet of Things.

Let me give you three specific examples of how AI can make business processes more efficient. AI can notably automate receipt allocations by intelligently matching receipts to payments. It can also assign and adjust customer credit ratings, allowing your business to assign different payment terms and strategies to each customer, and it can help establish customer-specific collection priorities and strategies, such as reserving more stringent collection practices for less strategic customers.

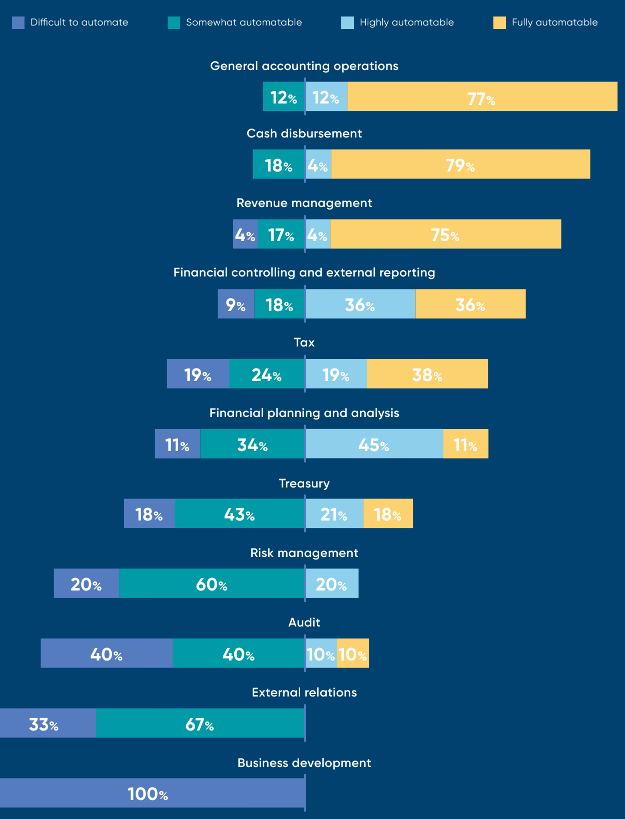
> “ Organizations can leverage continuous innovation and advanced technology already built into existing solutions

> “ I do not believe AI will be an 'application'. I believe it will be a capability integrated into all applications
>
> **Mark Hurd, CEO, Oracle**

AI can also automate and optimize many processes within the accounts payable function. Automatic invoice matching and allocation can reduce invoice holds by matching invoices to purchase orders and properly allocating them to the chart of accounts. AI can also inform early payment discounting or dynamic discounting programs by setting optimal rates for individual suppliers. It can also minimize supplier risk by drawing from third-party data, such as credit ratings, to help your company predict anomalies and negative conditions with suppliers before they become an issue for your inventory and production processes.



Transactional activities are the most automatable, but opportunities exist across most subfunctions.



[1] Proportion of tasks. Figures may not sum to 100%, because of rounding.

1 *ENTERPRISES WILL REVOLUTIONIZE APPS AND APPS WILL REVOLUTIONIZE ENTERPRISES*

By 2022 about 90% of apps will be built on microservices, which improve the ability to design, debug, update and leverage third-party code, providing applications that are much more complex. In turn, they will allow an organization to evolve its technology stack, giving it the means to install even better IT infrastructure. Not to mention that 35% of all production apps will be cloud native, making production speeds faster.

2 *DIGITAL INNOVATION WILL ACCELERATE IMMEASURABLY*

In the years spanning between 2019 and 2023, approximately 500 million new logical apps will be created, which is equal to the number of apps built over the past 40 years.

3 *SECURITY WILL BE REDEFINED*

By 2022, 50% of servers will encrypt data both at rest (inactive data stored on any device) and in motion (active data in transit). More than 50% of security alerts will be automatically resolved by AI, and no less than 150 million people will have a digital identity embedded in a blockchain-based system.

4 *FRESH INFLOW OF PROFESSIONAL DEVELOPERS WITH NEW SKILLS*

In 2024, a new class of professional developers will expand the current developer population by 30%. They will be able to produce code without custom scripting, therefore accelerating each company's digital transformation.

5 *AI WILL BE THE NEW UI*

2024 is the year in which one-third of today's screen-based apps will be fully automated and AI-enabled. The user interface (UI) will be maintained by artificial intelligence and as early as 2022, 30% of companies will engage with their customers using conversational speech technology.

WHAT WILL CHANGE IN THE NEXT 5 YEARS IN THE IT INDUSTRY?

International Data Corporation (IDC) published its worldwide IT industry 2019 top 10 predictions for the next five years. What's new and what will change? Here you get an overview of the five most important trends.

FIGHTING MACHINE-SPEED ATTACKS WITH AI

DARKTRACE

Cybercrime could cost the world as much as € 5,45 trillion annually by 2021, according to Cybersecurity Ventures' 2019 Cybercrime Report[1]. This represents the greatest transfer of economic wealth in history, surpassing the global trade of all major illegal drugs combined. As attackers learn to move at unprecedented speeds, organizations are embracing AI to regain the advantage over today's fast-changing adversary. Founded by mathematicians from the University of Cambridge and cyber intelligence experts, Darktrace offers a fundamentally different platform that is powering an entire cyber defense strategy with AI and machine learning. Hanen Ziad, PR Director, tells us how emerging technologies can help organizations keep pace with an ever-evolving cyber arsenal.

WHAT IS YOUR PERCEPTION OF THE CYBERTHREAT LANDSCAPE? ARE WE WITNESSING A CYBER WEAPONS RACE?

H.Z. We are indeed in the midst of a cyber arms race. Nation states around the world have increasingly turned to cyber weapons to garner intelligence, wield influence, disrupt their adversaries' infrastructure and major organizations, or cause serious physical damage. The US and UK security services have both warned that Russia's interference into critical infrastructure and major businesses is not something they can sit by and tolerate. Both are stepping up offensive strategies. For instance, the New York Times reported recently that the US government has implanted malicious code – for surveillance or attacks – into Russia's power grid[2]. However, most attacks remain faceless and many are not attributable.

BASED ON YOUR EXPERIENCE, HOW WILL CYBER RISK CONTINUE TO EVOLVE?

H.Z. Cyber-criminal activity is growing as it continues to pay handsomely to the perpetrators. Not only are humans unable to keep up with today's threat climate but AI attacks are approaching, where the computer code itself takes decisions on how to perform an attack – a self-driving attack. Only AI can fight AI and the best algorithms will win.

> “ Only AI can fight AI. The best algorithms will win

DARKTRACE ENTERPRISE IMMUNE SYSTEM IS SAID TO ACT SIMILARLY TO THE HUMAN IMMUNE SYSTEM. HOW DOES IT WORK?

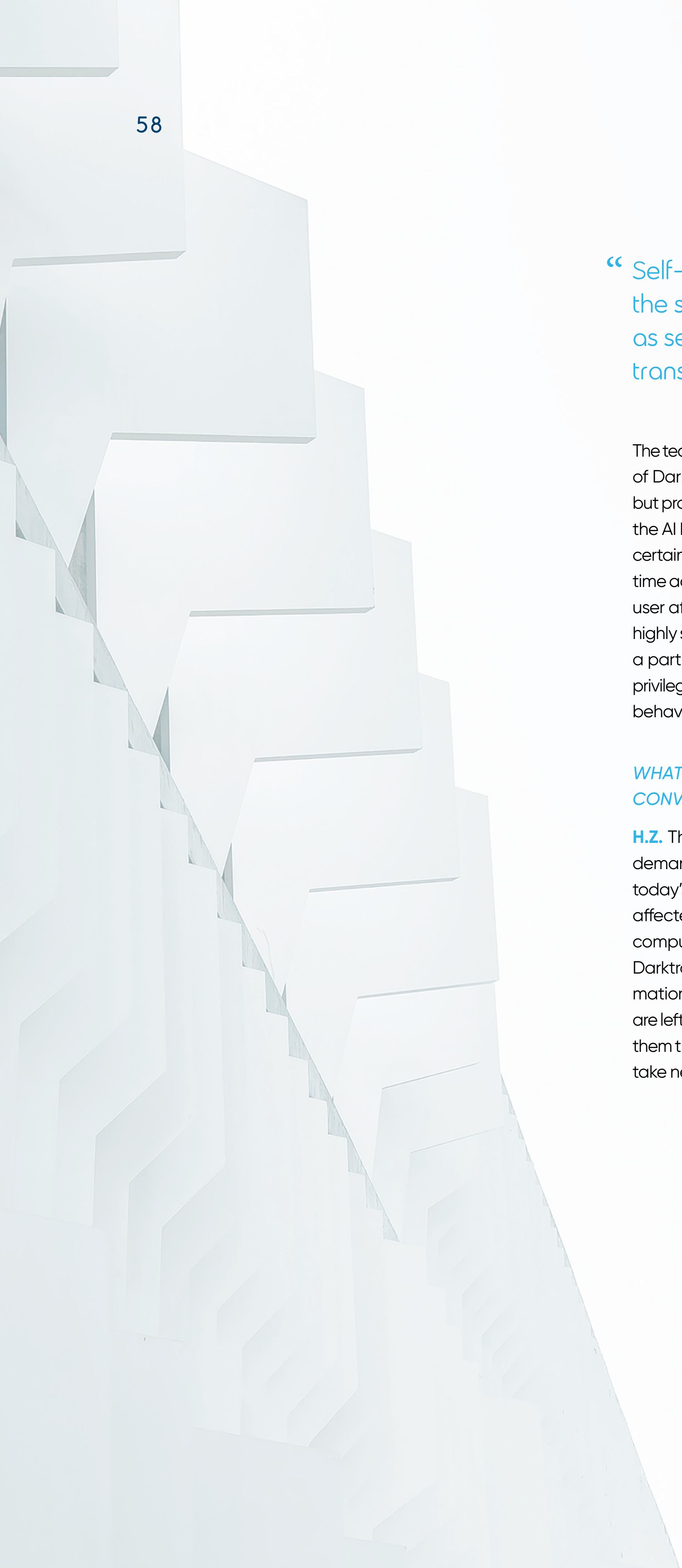
H.Z. Darktrace's foundational technology is based on unsupervised machine learning within a Bayesian mathematical framework, developed by mathematicians at Darktrace's Cambridge headquarters. These algorithms analyse network data at scale and make millions of probability-based calculations using the evidence they see. Instead of relying on knowledge of past threats, the algorithms understand the normal behaviour of every device and user - what we call the pattern of life - and detect significantly anomalous activity. Threats detected include corporate espionage, ransomware, insider data exfiltration and nation state attacks against critical infrastructure, to name a few.

Darktrace Antigena[3] represents a step forward in the development of the AI, as it offers, for the first time, the possibility of a self-healing network. Just as self-driving cars will revolutionize transportation, self-healing networks are changing the stakes for the security teams tasked with protecting critical data. Antigena is like an additional person on their team, protecting them from data breaches or attacks that they might otherwise have been too slow or unequipped to respond to, on a 24/7 basis.

[1] *Cybersecurity Ventures, "2019 Official Annual Cybercrime Report", December 2018*

[2] *The New York Times, "U.S. Escalates Online Attacks on Russia's Power Grid", June 15, 2019*

[3] *www.darktrace.com/en/products/antigena*



> “ Self-healing networks are changing the stakes for security teams, just as self-driving cars will revolutionize transportation

The technology works by harnessing the power and precision of Darktrace’s threat detection, to calculate an effective but proportionate response to an in-progress attack. Once the AI has identified threatening activity that surpasses a certain threshold of severity, its algorithms generate a real-time action that enforces the pattern of life of the device or user affected. These actions include interrupting specific, highly suspicious connections, automatically reconfiguring a part of the network or temporarily freezing certain user privileges. These surgical actions only target the threatening behaviour, while allowing business to continue as usual.

WHAT ARE THE ADVANTAGES COMPARED WITH CONVENTIONAL SOLUTIONS?

H.Z. This autonomous response technology is in urgent demand, given the increasing technical sophistication of today’s attackers. The 2017 WannaCry ransomware, which affected 30,000 organizations, is just one example of a computer-speed attack with massive reach – one that Darktrace identified in a matter of seconds. As more automation is employed by attackers, IT security professionals are left in the dark and outpaced. Darktrace Antigena buys them the required time to catch up with a major threat, and take necessary, longer-term actions.

WHAT INDUSTRIES OR SECTORS ARE LIKELY TO BENEFIT THE MOST FROM DARKTRACE'S SERVICES?

H.Z. Every modern business, regardless of size or industry, needs cyber security given the increasing scale and sophistication of threats. The Enterprise Immune System is inherently scalable. It can cover from two to ten million devices and so grows with the organization. Moreover, the Enterprise Immune System is appropriate for organizations in all industry verticals and uptake has been seen across retail, telecommunications, healthcare, government and defence, transport, energy and utilities, non-profit, legal, and financial services. Prominent customers include HSBC, Drax, Virgin Trains, BT, Metro Bank, T Mobile and Sunsweet Growers.

WHAT WILL BE YOUR NEXT TECHNOLOGICAL STEP?

H.Z. This month, we announced the launch of the Cyber AI Analyst, a new technology that emulates human thought processes to continuously investigate cyber-threats at machine speed. With the power to transform the security industry, early adopters of this technology reported at 92% reduction in the time required to investigate threats and provide conclusions to executives. This ground-breaking innovation is the culmination of over three years of research at the Darktrace R&D Center in Cambridge, UK. Using various forms of machine learning, including unsupervised, supervised, and deep learning, the technology learned human intuition and trade craft from more than 100 world-class cyber analysts across thousands of customer deployments.

> “ The Cyber AI Analyst is a new technology that emulates human thought processes to continuously investigate cyber-threats at machine speed

> “ 40% of Darktrace employees are women and many of them are fulfilling technical roles

WHAT ARE THE AMBITIONS OF DARKTRACE IN TERMS OF INTERNATIONAL EXPANSION?

H.Z. With AI attacks on the horizon, Darktrace's ambition is to continue helping organizations all over the world to build trust with artificial intelligence, preparing them to hand over the keys to the AI and allowing it to make critical decisions and take action where necessary.

DARKTRACE IS CO-CHAIRED BY TWO WOMEN, NICOLE EAGAN AND POPPY GUSTAFSSON, WHICH IS NOT THAT COMMON IN THE TECHNOLOGY INDUSTRY. HOW DO THEY EXPERIENCE THIS SITUATION?

H.Z. Nicole and Poppy are prominent examples of female CEOs who have helped build an organization that is leading the way in gender diversity across all levels of seniority. 40% of Darktrace employees are women and many of them are fulfilling technical roles, such as sales engineers and cyber analysts.

This has not been achieved with quotas, but instead through a hiring model that purposefully challenges the status quo of information security. Poppy and Nicole are champions of the idea that the sector does not only need artificial intelligence experts, but it needs problem-solvers, linguists, ethicists and artists too. Their advocacy for diversity in technology is important in an industry that tends towards under-representation of women and has driven Darktrace to do more to promote STEM subjects to girls and young women. Darktrace recently became a sponsor of WISE, a social enterprise that aims to increase female participation in science and technology . We are currently planning outreach on this topic with schools.

RECRUTER ET ACCOMPAGNER LES TALENTS

À L'ÈRE DU DIGITAL

Sur le marché des compétences digitales, la pénurie touche la quasi-totalité des métiers. Le phénomène n'est pas nouveau, mais il est aujourd'hui amplifié par la numérisation accélérée de l'économie et la montée en puissance des technologies de l'Intelligence Artificielle, du Big Data, de l'Internet des Objets et de l'automatisation, grandes consommatrices de ressources spécialisées. Pour rencontrer leurs objectifs de recrutement, les entreprises doivent désormais multiplier les initiatives. Patricia Bettembourg, Directrice des Ressources Humaines de Proximus Luxembourg, témoigne des efforts constants déployés par l'entreprise pour identifier, recruter et développer les nouveaux talents indispensables au succès de projets qu'elle conduit pour ses clients.

QUELS SONT LES PROFILS LES PLUS RECHERCHÉS AUJOURD'HUI ET DE QUELLES QUALITÉS PARTICULIÈRES DOIVENT-ILS FAIRE PREUVE ?

P.B. S'il y a 10 ans encore, nous évoquions les technologies de l'information et de la communication pour désigner notre activité, le digital leur a aujourd'hui clairement volé la vedette et dorénavant, ce sont des profils à forte expérience dans ce domaine que nous recherchons. La montée en puissance du digital, c'est-à-dire de l'ensemble des activités technologiques à destination des individus, a pour effet de redonner la main au client, de rendre le pouvoir à l'utilisateur. En conséquence, Proximus Luxembourg, à travers ses deux marques Telindus et Tango, se retrouve face aux fondamentaux de la relation client.

Patricia Bettembourg, *Directrice des Ressources Humaines de Proximus Luxembourg*

Aujourd'hui, nous recherchons des profils qui ne sont plus seulement techniques mais également largement orientés clients. Pour justifier la pertinence de nos services et prouver la qualité de nos produits, nous devons nous entourer de profils compétents d'un point de vue technologique mais aussi dotés de bonnes capacités relationnelles. En se développant, l'éventail des compétences nécessaires pour faire face aux enjeux du digital est devenu très complexe. La personnalité et le style de leadership que nous attendons de nos collaborateurs sont également d'un genre nouveau. La difficulté majeure est de trouver des profils polyvalents qui possèdent des compétences techniques poussées tout en étant flexibles, agiles et collaboratifs.

COMMENT LE DÉPARTEMENT RH DE PROXIMUS LUXEMBOURG ABORDE-T-IL LE RECRUTEMENT DE NOUVEAUX COLLABORATEURS ?

P.B. L'avenir de notre entreprise dépend fortement des talents dont elle dispose. Comme je viens de l'évoquer, nous avons besoin de professionnels pointus dont les compétences interpersonnelles - les soft skills – répondent aux besoins de nos clients. Trouver ces perles rares n'est donc pas chose facile, d'autant plus que les aspirations des jeunes professionnels ont considérablement évolué ces dernières années. Au-delà du package salarial, ils recherchent de la reconnaissance de la part d'une entreprise capable de susciter en eux un sentiment d'appartenance. Ils désirent également pouvoir établir une relation de confiance réciproque avec leurs managers. Je considère qu'aujourd'hui, nous recrutons non plus des ressources mais des talents qui attendent d'une entreprise qu'elle puisse leur offrir en permanence des possibilités de développement professionnel, des opportunités de mobilité interne et des occasions de relever de nouveaux challenges.

Les jeunes professionnels de la génération Z sont très sensibles à la valeur que l'on accorde à leur travail. Ils veulent se sentir utile, comprendre ce qu'on leur demande et trouver du sens à ce qu'ils font. Je suis convaincue que la reconnaissance est vraiment la clé pour retenir ces talents. Nous devons absolument en être conscients et y travailler à tous les niveaux de l'entreprise et de l'organisation.

DE QUELS LEVIERS D'ACTION DISPOSEZ-VOUS POUR RETENIR CES TALENTS AU SEIN DE VOTRE ORGANISATION ?

P.B. Chez Proximus Luxembourg, nous voulons offrir à nos employés un environnement qui soit propice à leur bien-être. C'est pour cette raison que nous avons créé un espace de convivialité au sein de notre nouveau bâtiment afin que nos collaborateurs se sentent immergés dans un esprit de collaboration et de convivialité.

A chaque fois que l'occasion se présente, nous plaçons nos employés sur le devant de la scène en valorisant les contrats remportés et les projets réussis à travers une communication adaptée. Renforcer le sentiment d'appartenance à l'entreprise de nos collaborateurs est un élément important à nos yeux et cela le devient de plus en plus. Pour cela, nous organisons des afterworks, des forums d'échange, des séances sportives ou encore des événements extra-professionnels. Maintenant que nous sommes bien installés dans notre nouveau bâtiment, ces initiatives vont aller en s'accélérant au cours des mois à venir.

Nous mettons par ailleurs à la disposition de nos collaborateurs un environnement dans lequel ils peuvent accroître leur capital compétences. C'est une clé essentielle pour la rétention des talents, d'autant plus dans un secteur d'activité comme le nôtre où l'évolution rapide des technologies exige une mise à jour constante des compétences.

Réputé pour son excellence technologique, Proximus Luxembourg est aussi une marque employeur qui constitue un précieux atout pour renforcer notre attractivité auprès des jeunes professionnels. C'est pourquoi le travail sur notre marque employeur est aujourd'hui un objectif majeur pour notre département RH. Il faut garder à l'esprit que 75% des professionnels sont des candidats passifs . Notre marque employeur nous permet d'être là où les candidats potentiels sont et d'atteindre ceux qui ne recherchent pas activement un nouvel emploi. Elle nous permet aussi de mieux fidéliser les talents que nous voulons retenir et de faire de certains d'entre eux de véritables ambassadeurs.

En ce sens, nous abordons aussi la gestion des carrières de manière personnalisée. Cela passe notamment par la mobilité interne: dès qu'un poste est à pourvoir, nous offrons à nos collaborateurs la possibilité de postuler, avant même de rechercher un candidat à l'extérieur de la société. Certains responsables de département sont parfois réticents à perdre ainsi un bon élément, mais la plupart ont compris qu'il valait mieux laisser partir un collaborateur talentueux vers un autre département de notre entreprise que de le voir nous quitter pour une autre société.

EST-CE QUE LA FLEXIBILITÉ QUANT AU LIEU DE TRAVAIL EST UN PARAMÈTRE QUI EST PRIS EN COMPTE CHEZ PROXIMUS LUXEMBOURG ?

P.B. Cette préoccupation commence à être prise en compte même si notre marge de manœuvre en la matière est encore limitée par certaines contraintes légales, fiscales et de sécurité sociale. Au Luxembourg, Proximus est un professionnel du secteur financier qui est tenu de respecter de bout en bout les règles fixées par la CSSF, notamment en matière de télétravail. Ceci dit, les dirigeants de la société et les délégués du personnel ont entamé une réflexion quant aux possibilités d'introduire progressivement plus de flexibilité dans les horaires de travail tout en respectant le cadre légal.

QUELS SONT VOS CANAUX DE RECRUTEMENT DE PRÉDILECTION ?

P.B. A l'ère du digital, nous avons bien sûr largement recours aux forums professionnels et aux réseaux sociaux, LinkedIn en particulier, mais nous participons également activement aux salons de recrutement afin d'assurer une présence soutenue sur le terrain. Nous avons d'ailleurs récemment étoffé notre équipe de recruteurs. Et lorsqu'il s'agit de trouver certains profils particuliers, nous travaillons avec des cabinets spécialisés.

D'autre part, nous encourageons de plus en plus nos collaborateurs à jouer un rôle d'agents de recrutement et d'ambassadeurs de la qualité de l'emploi chez Proximus Luxembourg. La cooptation est une formule qui fonctionne bien et qui nous apporte une garantie supplémentaire quant aux compétences du candidat qui nous est recommandé.

Enfin, l'émergence de technologies comme le Big Data, l'Intelligence Artificielle ou l'Internet des Objets nous confronte à des métiers nouveaux et des défis inédits. Nous sommes en train d'adapter nos méthodes de recrutement à ces profils qui ne sont pas nécessairement issus des filières habituelles et qui nous poussent à repenser notre approche de la recherche de talents.

LE SAVOIR NE FAIT PLUS LE POUVOIR

Selon le World Economic Forum, deux tiers des emplois actuels n'existeront plus en 2030. Motif : l'émergence de technologies qui automatisent le travail courant et répétitif à la vitesse grand V.

En s'arrogeant les tâches monotones et répétitives, la technologie nous oblige à miser sur la créativité. Les plateformes numériques comme YouTube et Instagram, qui reposent entièrement sur la créativité de leurs utilisateurs, sont là pour le prouver. Au même titre que la réalité virtuelle, bel exemple de technologie liée à l'imagination humaine.

> “ Dans l'économie de l'imagination, la pensée intuitive et créative génère une valeur économique.

OUTSOURCING DE LA PENSÉE RATIONNELLE

Nous sommes à la veille d'une ère nouvelle : celle de l'économie créative ou économie de l'imagination, dans laquelle la pensée intuitive et créative génère une valeur économique et nous externalisons la pensée logique et rationnelle pour la confier à l'automatisation.

Une étude de McKinsey révèle que le travail physique prévisible ainsi que la collecte et le traitement des données seront les premiers à céder à l'automatisation. Les tâches les moins technologiquement compatibles sont la prise de décision, la planification, l'interaction humaine et le travail créatif domaines où l'homme continue à dominer la machine. Nous pouvons donc en déduire que les créateurs, concepteurs et développeurs de produits et services en tout genre seront de plus en plus courtisés.

LE POUVOIR DE L'IMAGINATION

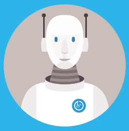
Survivre dans l'économie créative exigera de nouvelles aptitudes. Le pouvoir ne sera plus une question de connaissances mais de créativité. L'imagination et la créativité ne relèvent pas exclusivement de talents innés : ce sont des compétences qui s'apprennent et se stimulent. Cette nouvelle économie ne se limitera évidemment pas aux seules fonctions créatrices ou rédactionnelles ; les entrepreneurs, scientifiques, managers, comptables ou experts IT devront aussi se montrer créatifs. Une évolution dont il convient de tenir compte dès aujourd'hui dans l'enseignement et les formations. Tout comme nous avons, par le passé, privilégié le renforcement du savoir dans l'économie de la connaissance, nous devons aujourd'hui faire du renforcement de la créativité un objectif prioritaire.

L'imagination et la créativité nous permettront de donner bientôt un sens nouveau à nos emplois, à notre activité économique. Le pouvoir de l'imagination se révèle aussi dans sa capacité à inventer une vision d'avenir et à la construire. "La logique vous mènera du point A au point B mais l'imagination vous mènera partout", disait Einstein. Une théorie plus que jamais d'actualité à l'ère de l'imagination et de l'économie créative.

11 hot jobs in 2025

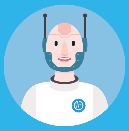
Coach RV

Équipe virtuelle dans bureau virtuel cherche coach H/F spécialisé, en chair et en os, pour la gestion des ressources humaines en réalité virtuelle.



Opérateur de drone

En tant que 'drone manager', vous gérez le planning et l'exécution des vols dans des domaines aussi divers que la logistique, l'étude scientifique, la production cinématographique...

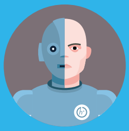


Project manager

Le travail par projet remplace les tâches fixes d'un passé proche. Les project managers coordonnent les projets et assurent la liaison entre les collaborateurs indépendants.

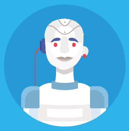
Expert en philosophie des technologies

Intelligence artificielle, apprentissage automatique et autres nouvelles technologies ont un énorme impact sur l'homme et la société. L'expert en philosophie des technologies étudie l'éthique liée à leur utilisation humaines en réalité virtuelle.



Conseiller en cryptofinance

Bienheureux ceux qui afficheront, sur leur CV, des compétences en sécurité IT et management financier. Ils géreront le portefeuille de cryptomonnaie des entreprises et particuliers en réalité virtuelle.



Mentor médical

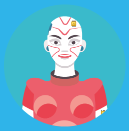
Code rouge ! L'app qui contrôle votre pression artérielle bipe : votre tension est trop élevée. Heureusement, en 2025, vous pourrez compter sur un mentor médical pour une interprétation et un accompagnement professionnels du suivi de votre santé.

Serrurier numérique

Le serrurier se met à l'heure numérique. En cas de dysfonctionnement technologique, le serrurier numérique vient à la rescousse des personnes qui se retrouvent coincées, le plus souvent dans leur voiture ou chez elles.

Technicien en domotique

Un électricien ne vous aidera pas à résoudre vos problèmes d'éclairage par commande vocale. Comme la domotique et l'IoT équipent désormais nos maisons, les coordonnées d'un technicien en domotique pour la connexion et la sécurisation de vos appareils seront utiles.

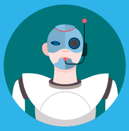


Coach en productivité personelle

H/F expert en concentration. Si l'automatisation nous soulage des tâches répétitives, il en est d'autres qui restent de notre responsabilité. Mais l'essor des technologies tend à nous distraire, réseaux sociaux en tête. Le coach en productivité personnelle veille sur votre concentration.

Formateur numérique

L'évolution technologique galopante exige une mise à jour constante des compétences chez tous les travailleurs. Les cours, formations, tutoriels ou encore webinaires sont de plus en plus souvent organisés en ligne.



Concepteur 3D

Hamburgers, chaussures, prothèses : les concepteurs en impression 3D sont présents dans quasiment tous les domaines. Et leur rôle ne se limite pas à changer les pièces des machines... Quelle est votre taille ?

AFTER-WORD

CLOTHES? WITH ALL THIS WEARABLE TECHNOLOGY I DON'T HAVE ROOM FOR CLOTHES!!!

Millenials & IOT, the perfect match ?

Millennials: the generation that is just old enough to remember the years without the internet, with Sony Walkmans, music cassettes and Windows 95. And the generation that is, at the same time, young enough to have experienced the digital wave since childhood. The so-called millennials ... I'm one of them. A 'late' one, admittedly. In my early twenties, a newcomer on the labor market and a digital native. But how do we, the millennials, deal with the digital reality? Do we embrace the Internet of Things (IoT) just like that?

I do, at least. The idea that everything is connected to everything, all the time and everywhere, does not scare me. On the contrary, I benefit fully from the convenience provided by IoT. It doesn't stop with the smartphone any longer. Wireless headphones, an Apple TV and Chromecast, smart speakers, smart lamps, locks and doorbells and so on, they are all part of my daily life. And if – in exchange for all this convenience – I have to give up some of my privacy, well, then so be it. Here's a small example: Recently, I was sitting on a tram in the center of Ghent when suddenly I got a message on my smartphone. "Come along and see us", it said. "We're just around the corner." Sender: Nespresso. I knew straight away where I could find my favorite brand of coffee. And when I actually went into the shop, I was offered a free coffee spontaneously. Marketing tricks? Certainly! But it did make me happy. And without my smartphone, I might well have just gone to my usual coffee bar. That's nearby too, but the coffee there isn't for free. You see: being connected all the time has its advantages.

But when I compare my attitude with that of my contemporaries, I notice that IoT isn't so warmly welcomed by everyone. A lot of people don't want to spend money on expensive, unnecessary gadgets. Take the smartwatch, for instance: more expensive than the average wristwatch, but what added value does it really offer? It would be better to keep the money to go out for a meal, or travel – because millennials usually travel more than their parents ever did.

Others have concerns about the impact of IoT on our privacy. IoT applications need our data, and people don't like giving it away. And if there really is no other option, then people at least want shared data to be secure. So security services will definitely play a role in the further development of IoT applications. Whether we like it or not, the IoT will prove even more useful in the future. At the moment mainly in our private lives, but soon also – and above all – in public places and in the business world. No more driving around endlessly until you come across a parking space, but finding a free space straight away via an app. No more lighting all the streets all night, but lamps that only light up when someone passes by. Handy, right? Just look at the smartphone: 10 years ago, virtually no one had one. "Not necessary", they said. Now, no one can do without them. For IoT it may not be any different.

JASON SAMPERS,
Segment Marketing Analyst at Proximus

You see a device.
We see secure access to the enterprise.
mobileiron
The center of enterprise security

NetApp
DISTRIBUTION PARTNER

Data center nouvelle génération

Etes-vous prêt ?

Bénéfices pour votre business

Performances garanties
Déployez vos applications avec la certitude qu'elles s'exécuteront de façon optimale.

Flexibilité et évolutivité
Faites évoluer votre infrastructure à votre rythme.

Infrastructure automatisée
Transformez vos opérations IT.