ACADÉMIE DES TECHNOLOGIES
POUR UN PROGRÈS RAISONNÉ CHOISI PARTAGÉ

LA CYBERSÉCURITÉ ET LES ENTREPRISES : UNE VISION DE TERRAIN

Jean-Luc Moliner
Membre de l'Académie des technologies

Séance du 6 juillet 2022

Résumé

La cybersécurité est malheureusement un sujet d'actualité, les événements en Ukraine l'ont rappelé récemment. Elle concerne désormais aussi bien les États que les entreprises et les particuliers. Face à des menaces et des attaques de plus en plus nombreuses, de plus en plus sophistiquées, de plus en plus agressives et destructrices, chercheurs, ingénieurs, fabricants de logiciels, testeurs, développeurs, directeurs cybersécurité au sein des entreprises et des administrations…, toutes les forces se mobilisent pour construire une défense commune et efficace. Au lendemain du Forum International de la Cybersécurité 2022, qui a souligné les efforts faits et à faire dans le contexte géopolitique d'aujourd'hui, l'Académie a donné la parole à des acteurs du monde de l'entreprise impliqués dans cette guerre sans merci, pour aborder des problématiques qui touchent désormais tout le tissu économique. Pourquoi est-il si difficile, à l'échelle industrielle, de fabriquer du logiciel sûr ? Faut-il allier les savoir-faire de la DGSE et la combativité des forces spéciales pour diriger la cybersécurité d'une grande entreprise ? Quelles sont les méthodes de la cyber mafia ? Les hackeurs auront-ils toujours un temps d'avance sur nos capacités de défense ? Réponses pragmatiques de quatre acteurs en prise directe avec l'ennemi.

Intervenants

Marion Videau
CTO de Quarkslabs

Jean-Yves Poichotte
Responsable de la sécurité des systèmes d'information (RSSI) de Sanofi

Denis Pélanchon
Directeur général de Cartesian Lab

Nicolas de Rycke
Associé co-fondateur de la société Axis&Co et enseignant à l'école de guerre économique

Sommaire

Pourquoi est-il si difficile de fabriquer du logiciel sûr ?

Marion Videau

Marion Videau, après avoir enseigné à l'université de Lorraine et travaillé pour l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), est aujourd'hui responsable scientifique de Quarkslab, une société d'évaluation et d'édition de logiciels. Son exposé est le résultat de réflexions communes avec d'autres membres du bureau recherche et technologie de Quarkslab : Ivan Arce, Damien Aumaitre et Béatrice Creusillat.

L'impasse théorique

Sur le plan théorique, nous ne disposons pas de programme applicable à des systèmes complexes pouvant garantir l'absence de certaines vulnérabilités. Alors qu'on fabrique du logiciel en empilant de multiples couches de logiciels, rien ne garantit qu'assembler deux éléments dans lesquels on peut avoir raisonnablement confiance donne un résultat qui soit « sûr ».

La sécurité n'est pas une propriété simple. Pour emprunter au vocabulaire de la théorie des systèmes complexes, c'est une « propriété émergente », un peu comme la conscience chez les êtres humains.

Limites du champ des possibles

Nous produisons chaque année beaucoup plus de processeurs que ne naissent d'humains dans le monde, non sans nous heurter à des limitations pratiques assez fondamentales.

Premier écueil, les processeurs généralistes dont la puissance augmente de manière exponentielle ne font quelque chose de moins universel que parce qu'on les programme pour cela. La simplicité étant obtenue à partir de la complexité, on s'expose à plus de « vulnérabilités ».

Second problème, il y a entre le langage de programmation « de haut niveau » utilisé par le concepteur de logiciel et le langage machine des processeurs et équipements informatiques tout un processus de traductions successives qui ne sont pas toujours maîtrisées.

Par ailleurs, les logiciels d'aujourd'hui sont construits à partir d'une base logicielle commune et intègrent beaucoup de briques de logiciel de provenances diverses. On se retrouve forcément avec de grosses zones d'ombre.

Enfin, la manière dont on assemble des modules supposés « sûrs » peut elle-même être source de vulnérabilités. Or, il est essentiel d'assurer la cohérence de tout le système.

Trop peu de motivation pour la sécurité

Pour autant, mise à part la DGA qui achète du logiciel pour cet usage, les parties prenantes de notre marché sont nombreuses et ne se soucient pas suffisamment de sécurité. Or les acteurs qui vont subir les conséquences d'un logiciel vulnérable ne sont pas seulement ceux qui l'achètent. Et ceux qui vont être impactés ne sont pas toujours prêts à payer le coût d'une meilleure sécurité.

En fait, personne ne mentionne dans son cahier des charges des exigences négatives. Pourtant la sécurité exigerait de le faire. La plupart du temps, le logiciel est testé par ses développeurs. Or ceux-ci sont plus enclins à prouver que le logiciel a les fonctionnalités positives requises qu'à chercher les failles et les limites de leur « bébé ». Il serait plus efficace d'avoir des testeurs indépendants, mais peu de sociétés peuvent se permettre d'avoir une équipe distincte de développeurs et de testeurs.

Des pistes pour demain

En dépit de ce panorama peu engageant, il est indéniable que d'énormes progrès ont été faits. Le matériel est plus sûr, on commence à automatiser les analyses, on dispose de langages qui ont, par défaut, des fonctionnalités de sécurité grâce aux méthodes formelles permettant de fournir des preuves de sécurité. C'est bien mais ce n'est pas suffisant pour faire face à la quantité croissance de logiciels, de complexité… et d'attaques. Il faut automatiser davantage, et surtout travailler ensemble, créer des interactions constructives entre domaines technologiques, business, règlementation, recherche... Aucune amélioration ne viendra d'un seul de ces acteurs.

Outils, méthodes et ressources disponibles dans une grande entreprise pour un responsable sécurité des systèmes d'information

Jean-Yves Poichotte

Jean-Yves Poichotte est directeur de la cybersécurité du groupe Sanofi depuis huit ans. Diplômé de l'École des Hautes Études Industrielles, il a été pendant 7 ans directeur de la sécurité de l'information des fraudes du groupe SFR. Ses missions l'ont amené à travailler régulièrement avec l'ANSSI et divers services de l'état.

Sanofi est une société française présente dans 90 pays, ce qui signifie pour le patron de la cybersécurité : 90 cultures différentes à couvrir, 90 régulations, 90 écosystèmes géopolitiques… Elle regroupe 25 000 personnes en France et 95 000 collaborateurs dans le monde. Et comme beaucoup d'entreprises, Sanofi consomme de plus en plus d'informatique, ce qui représente une grande opportunité de croissance mais aussi un enjeu de sécurité essentiel. En outre, le groupe Sanofi est le résultat de 80 fusions et acquisitions. Tous les ans, il intègre 3, 4, 5 nouvelles entreprises qui ont chacune des fragilités informatiques, éventuellement des compromissions. Certaines ont déjà été pénétrées et prises sous contrôle des attaquants. Lorsque vous les connectez à votre entreprise, vous héritez de tout cela… La guerre en Ukraine n'a fait que révéler la complexité de notre métier.

Pourquoi on attaque Sanofi ?

On pourrait imaginer qu'on attaque Sanofi pour voler des informations. Un laboratoire pharmaceutique est doté de secrets, de brevets... Sauf qu'un laboratoire publie ses recherches et ses travaux continuellement, le tout étant régulé et validé par les autorités de santé du monde. Ce qui, en revanche, est extrêmement secret, ce sont nos fusions acquisitions. Quand on veut acheter une entreprise, le prix aujourd'hui tourne autour de plusieurs milliards, et peut doubler instantanément si on est deux à se battre pour la même start-up. Ça, on le protège ! C'est stocké dans des systèmes français très sécurisés.

Le risque essentiel, en fait, c'est l'accident industriel sur nos chaînes de de production, qui concourrait à créer une rupture dans la continuité d'approvisionnement. On entre, par exemple, dans notre usine de fabrication de vaccin contre la grippe, au bon moment, et on arrête l'usine suffisamment longtemps - 2 ou 3 semaines - pour nous empêcher de lancer le vaccin. On imagine le dégât que cela ferait en Europe !

Une défense en mode commando

Si le métier se limitait autrefois à définir des règles et à les appliquer, aujourd'hui, face à des attaquants extrêmement agressifs, notre organisation cybersécurité est conçue sur le modèle des forces spéciales : très compacte, extrêmement concentrée, multi-polyvalente, répartie sur tous les pays mais autour d'une seule organisation et une seule politique de cybersécurité.

Nous sommes attachés à la Direction Digitale du Groupe mais le Comité de Direction de Sanofi considère que notre activité est le seul métier du groupe qui n'a pas de frontières. Partout à travers le groupe, nous sommes donc légitimes sur tous les sujets liés à la sécurité, mais devons aussi nous préoccuper de ce qui se passe chez nos partenaires, éventuellement dans les états ennemis.

Dans ce nouveau contexte, les règles de base n'ont pas changé mais nous avons ajouté des radars. Comme sur l'autoroute : des systèmes qui viennent capturer tous les jours 400 millions de données sur le statut cybersécurité de nos 160 000 équipements. Quelle que soit la sécurité et la solidité de votre défense, une fragilité suffit pour que la totalité de l'entreprise soit détruite. 400 millions de données chaque matin c'est 400 millions de possibilités de pas être conformes à l'état de l'art !

L'année dernière, grâce à l'ensemble de nos systèmes de sécurité, nous avons bloqué automatiquement 11 millions d'événements - pas tous méchants -. Et mes équipes ont eu à réagir à un peu plus de 9 000 attaques sophistiquées dans l'année écoulée. Concrètement, nuit et jour, 365 jours par an, j'ai 22 attaques en moyenne à traiter instantanément, le plus vite possible.

En général, on arrive aujourd'hui à retrouver un niveau de sécurité satisfaisant après l'attaque en moins d'une journée.

La stratégie de combat

Notre première mission consiste à bâtir des murs. Tous les matins, j'envoie des soldats vérifier que les murs ne se sont pas effondrés pendant la nuit et que personne n'a oublié de de fermer la porte à clefs. Et je place des détecteurs et des équipes de réaction rapide partout. La Direction Générale nous a donné un mandat nous permettant de couper n'importe quel composant du système d'information en cas d'attaque : une machine, un service, une usine, un pays… Avoir cette liberté responsabilise mes hommes et nous donne un champ d'intervention exceptionnel.

En 2019, au début de la pandémie, nous avons pu stopper en deux jours une attaque. Certes, l'attaquant avait déjà visité 18 000 machines et n'était pas loin de nous voler des documents, mais il n'a pas réussi. Ce mandat qui permet de répondre vite, fort et de façon raisonnée, nous a permis de sauver l'entreprise.

Nouvelles zones de risques, nouvelles missions

Les attaques autrefois visaient à voler des secrets, aujourd'hui elles visent à détruire l'entreprise : geler les processus en chiffrant les données et en cassant les systèmes d'information, puis demander de l'argent en échange de la restitution des données. Elles sont le fait de de bandes criminelles à qui elles rapportent plusieurs milliards d'euros par an. Il arrive aussi que des états soient aux commandes, pour des raisons géopolitiques. Un nouveau pan de notre métier consiste donc à réfléchir, au-delà de la capacité du système à ne pas se faire attaquer ou à ne pas tomber, à la reconstruction : si on se fait détruire, comment est-ce qu'on reconstruit ?

L'autre nouvel enjeu, c'est d'envisager que la matérialité du risque pour Sanofi, c'est d'abord Sanofi : nous, nos salariés, nos systèmes d'informations, nos carences, nos faiblesses… Aujourd'hui 50% de nos activités sont sous-traitées. Ce qui est une tendance générale dans toutes les entreprises. Or, un fournisseur est un risque quand il héberge des données sensibles pour nous. Il est aussi un risque car plus aucun fournisseur ne travaille sans informatique. La dépendance au numérique, due à la digitalisation - légitime mais pas toujours raisonnée - de l'économie française a engendré une nouvelle zone de risque. Il faut donc développer nos radars, être capables de détecter le moindre mouvement.

Et puis nous devons recruter ! Certes, nos moyens humains sont en croissance mais c'est loin d'être suffisant. La frugalité est le lot des équipes cybersécurité en France. Ce qui est en train de créer une zone de vulnérabilité essentielle. Cela fait partie de nos nouveaux « challenges » : familiariser et intéresser à nos métiers les jeunes générations, notamment la population féminine, ainsi qu'une frange de gens compétents mais effrayés par le nouvel environnement Cloud.

Et demain ?

Nous ne gagnerons pas la guerre économique sans prendre de risques, sans investir dans de nouvelles technologies. Moi, le patron cybersécurité autrefois connu comme « monsieur Non » (« tu ne peux pas faire ceci, pas faire cela… »), je dois être aujourd'hui celui qui rend les choses faisables. Est-ce que l'entreprise doit partir sur le Cloud ? Oui. Mais pas n'importe comment. Est-ce qu'on peut acheter de la technologie américaine ? Oui. Chinoise ? Oui. Je dois faire le grand écart : protéger Sanofi occidental et Sanofi oriental.

Autopsie d'une compromission durable et silencieuse

Denis Pélanchon et Nicolas de Rycke

Denis Pélanchon, après une carrière d'officier dans l'armée de terre et 30 ans d'expérience en SSI (sécurité des systèmes d'information), est aujourd'hui directeur général de Cartesian lab, la filière qui porte les activités cybersécurité du groupe Altum.

Nicolas de Rycke est associé co-fondateur de la société Axis&Co, spécialisée dans le renseignement et l'investigation, et enseignant à l'école de guerre économique depuis 25 ans. Pratiquant de l'OSINT (open source intelligence), il a été développeur, administrateur de systèmes, réalisateur de tests d'intrusion…

Les cyberattaques sont aujourd'hui analysées, décrites, chiffrées. D'après une estimation de l'ONU, elles pourraient nous coûter 5 200 milliards de dollars sur les trois prochaines années. Tous ces chiffres sont bien sûr contestables, d'autant qu'ils ne concernent que ce qui a été vu et détecté… En tout cas, il s'agira d'attaques ciblées et sophistiquées. L'objectif de la cyber mafia étant de faire de l'argent, avec parfois une vraie approche marketing. Certains attaquants, une fois qu'ils ont repéré des vulnérabilités techniques, observent leur

cible, ses capacités, et vous demandent des rançons importantes en vous disant : « on a regardé vos chiffres, vos actionnaires, vous pouvez. » On a l'impression de discuter avec un commercial !

Les grandes étapes d'une cyberattaque

Avec les capacités dont on dispose aujourd'hui en recherche en source ouverte, il est très simple pour un attaquant d'obtenir beaucoup d'informations sur une cible potentielle. Au plan technique d'abord, parce que notre simple présence sur le réseau, la façon dont nos objets sont connectés et paramétrés en matière de sécurité, peuvent révéler un grand nombre de ressources, et donner des idées. Mais il peut également s'informer sur des acteurs de second rang qui travaillent au profit de cette entreprise.

L'Open Source Intelligence (l'OSINT) est forcément un outil quand on veut conduire une attaque ciblée. Nous l'utilisons nous-mêmes lors des tests d'intrusion où il s'agit justement de se mettre dans la peau de l'ennemi pour révéler à un client tout ce qu'on peut trouver lui, ses zones de fragilité, les scénarios qu'on pourrait mettre en œuvre pour l'attaquer…

Phase numéro 2 : une fois qu'il a réussi à prendre pied dans un premier élément du système d'information de sa cible, l'attaquant observe ce qui se passe à l'intérieur de l'entreprise afin de détecter d'autres ressources qui potentiellement, parce qu'elles seraient moins exposées, seraient peut-être moins protégées.

Et progressivement, il progresse au travers de flux légitimes dans le système d'information. Ce qui devient difficile à détecter. À moins d'avoir bien défini au préalable ce qui est autorisé et interdit comme circulation dans le système. D'autant que c'est dans cette phase-là que l'attaquant, qui ne dispose pas de panneaux indicateurs sur sa route, peut « faire du bruit ».

Il cherche donc, et à un moment, il va trouver. Si son but est la destruction, on le sait vite : quelque chose s'arrête. Mais s'il vise l'ingérence, c'est plus difficile car il va passer par la messagerie électronique, le composant du système d'information par excellence, qui contient des giga-octets de données, et auquel il peut aussi avoir accès depuis l'extérieur. En face, il faut être en capacité de détecter des connexions illégitimes. C'est très compliqué.

Itinéraire bis : la voie de la chaîne logistique

Mais il existe un chemin beaucoup simple pour forcer avec un minimum d'efforts l'accès à un maximum de cibles. Il consiste à infecter, en y introduisant un cheval de Troie, un logiciel utilisé par tous les clients. À la première mise à jour (c'est là qu'ont été implantés les « backdoors »), le cheval de Troie déploie ses forces sur toutes les cibles visées.

L'exemple le plus médiatisé de ce genre d'attaques « via la voie logistique » est celui de l'entreprise SolarWinds, un éditeur de logiciels, notamment des logiciels de supervision de réseaux informatiques, qui compte parmi ses clients 80% du *Fortune 500* aux États Unis, des administrations, des écoles, de très grandes entreprises… Récemment, un groupe d'attaquants motivés - en l'occurrence les services de renseignements russes - a réussi à pénétrer et prendre le contrôle complet de l'entreprise, puis à identifier un logiciel très intéressant qui permet de faire de la supervision en réseau. 30 000 clients touchés ! L'impact était considérable. Les mises à jour infectées dataient de 2019 et 2020, et l'attaque n'a été révélée au grand jour qu'en 2021 ! Exemple type d'une « compromission silencieuse et durable ». Extrêmement redoutable et très difficile à contrer parce que notre dépendance au logiciel et donc notre surface d'attaque sont énormes.

Rien de bien nouveau, en fait. En 1990 déjà, Kevin Mitnick, l'un des premiers hackeurs, devenu mythique dans le monde de la sécurité informatique, avait compris qu'en volant des codes sources de logiciel, il allait pouvoir étendre son emprise. Son jeu étant de contrôler le maximum de serveurs possible. La NSA elle-même n'est pas étrangère à ces pratiques… La liste serait longue de tous les éditeurs et autres fabricants de matériel, impactés de cette façon.

Un jeu d'enfants ?

Les cas de « state-sponsored attacks » (attaques sponsorisées par des états) comme celui de SolarWinds auraient tendance à nous laisser imaginer qu'il s'agit là de stratégies hautement sophistiquées conduites par des experts. Des exemples très récents nous ont prouvé le contraire. En début 2022, Lapsus, un groupe de hackeurs, a fait trembler la planète en s'attaquant à des cibles de tout premier plan. À commencer par la société Nvidia, premier fabricant de processeurs graphiques, à qui ils ont réussi à voler des codes sources, une propriété intellectuelle extrêmement importante. Puis ils ont menacé – technique classique du « ransomware » - : « Si vous ne payez pas, on distribue ». Et ils ont distribué le code source sur internet. Même chantage avec Microsoft (37 Giga de codes sources divulgués), avec Samsung, avec la société Okta qui fournit des systèmes de double authentification, avec T-Mobile, etc, etc.

Or, nous sommes loin ici de la « state-sponsored attack ». Lapsus n'était autre qu'un groupe d'ados : les deux principaux protagonistes arrêtés (ils ne faisaient pas dans la finesse et avaient laissé beaucoup de traces en quelques mois) avaient 16 et 17 ans. Et comme l'ont

prouvé des « chats » rendus publics, leur seul but était de s'amuser.

Comme quoi, un petit groupe d'acteurs motivés - sans contrainte de temps, sans éthique et sans limites - peut réussir à faire trembler des géants en termes de sécurité informatique. Avec un mode de fonctionnement très simple. Ils avaient posté des annonces sur la messagerie Telegram (« on recrute des employés prêts à vendre leur code d'accès » …) : une méthode pour pouvoir entrer chez une cible, rebondir sur une autre, et créer une sorte de cercle vertueux du piratage. Le piratage est aussi addictif qu'une drogue…

Nous avons toutes les semaines la démonstration qu'attaquer des librairies logicielles pour pouvoir mener des « supply-chain attacks », c'est trivial. Et c'est un problème très difficile à régler.

Les stratégies de défense

Tout n'est pas perdu pour autant ! Il est important, tout d'abord, d'accepter l'idée que l'un des composants présents dans une zone de confiance puisse être compromis, et construire de multiples lignes de défense. Limiter notamment la surface d'exposition de ses ressources, y compris celles qui ne sont pas dans le cœur de métier de l'entreprise.

Débats

L'augmentation croissante du nombre d'attaques n'est-elle pas à mettre en partie sur le compte de la standardisation des outils logiciels ?

Marion Videau : C'est vrai, la standardisation peut fournir des indications aux attaquants, surtout quand ils n'ont pas une cible précise, et que leur but est d'attaquer quel que soit le système. Mais les gens qui utilisent des logiciels ne restent pas non plus les bras croisés ! Nous développons à Quarkslab une solution de protection des applications dont un des effets secondaires rend beaucoup plus difficile pour un attaquant d'analyser le produit et de trouver des failles.

Le concept de TEE (Trusted Execution Environnement) peut-il avoir de l'avenir dans sa mise en œuvre pratique par l'ensemble des grands systèmes ?

Marion Videau : Oui et non. Tous ces nouveaux mécanismes de sécurité déplacent, en fait, la barrière du coût. Lorsqu'on fait des analyses de sécurité d'environnement TEE, on trouve régulièrement des vulnérabilités, mais cela représente des centaines de jours de travail d'une équipe d'experts… Alors oui, on a envie de relier un certain nombre de nos mécanismes de protection à un TEE et de savoir précisément quelle sécurité on apporte à nos clients, mais à quel coût ? Donc j'y crois, oui, c'est une vraie tendance de fond. Mais on ne peut pas affirmer que c'est la panacée.

Le déficit en ressources humaines peut-il conduire la cybersécurité à devenir dépendante d'un recrutement uniquement externe à la France ?

Jean-Yves Poichotte : Le risque n'est pas là, car tous les pays ont le même déficit. Le vrai risque, à échéance de 4/ 5 ans, serait de ne pas avoir les épaules collectives assez solides en Europe pour faire face à une vraie bataille cyber très méchante, celle que tout le monde redoute. Si 500 000 ou 1 million de machines et 50 entreprises sont attaquées en même temps, on ne saura pas faire face. On peut s'aider mutuellement, grâce au réseau et à la confiance, on est capable de se prêter des ressources, mais quand on sera tous à genoux, cela ne suffira pas.

Comment peut-on contrôler la loyauté des collaborateurs d'un service de cybersécurité ?

Jean-Yves Poichotte : Chez Sanofi, les salariés cybersécurité - qui sont les plus aptes à prendre le contrôle - sont des français « screenés » par la DGSI, des américains - les vaccins qu'on commercialise sont vitaux pour eux -, des mexicains -excellents et pas chers -, et des chinois parce que Sanofi en Chine représente 13 % du Chiffre d'Affaires, soit 6 milliards d'euros : on ne peut pas considérer la Chine comme un ennemi. Mais c'est un vrai problème. Alors, on se monitore. Et au-delà de ça, nous sommes en train de lancer un programme « insider-threat » pour tenter de « profiler » nos salariés qui ont des postes importants ou à risques. La pratique est assez courante dans les entreprises anglo-saxonnes mais nous sommes encore frileux, on ne fait que démarrer.

Au rythme d'une innovation toutes les heures et d'une start-up qui se crée tous les jours… Quelle place fait Sanofi à l'accueil des nouveaux entrants ?

Jean-Yves Poichotte : Nous avons besoin d'innovations, et en tant qu'entreprise française, besoin encore plus d'innovations françaises. Chez Sanofi, nous sommes des architectes de services cyber. Nous n'avons pas de bureau de recherches en cyber mais nous sommes connus pour avoir du flair sur les start-ups. Nous avons été le premier client d'Alcide, d'Acuity et d'un certain nombre de start-ups. Nous leur avons ouvert la totalité de notre réseau pour leur permettre de consommer notre base installée (30 milliards de données aujourd'hui) et d'améliorer leurs outils. En fait, ce n'est pas parce que c'est français qu'on achète, c'est parce que c'est français et prometteur.

Est-ce que les attaques visent autant les particuliers que les entreprises ?

Denis Pélanchon : Il faut combattre l'idée fausse : « je suis un petit individu dans mon coin qui n'intéresse personne ». Un attaquant est opportuniste, dès qu'il peut prendre un compte, il peut peut-être rebondir. Il faut donc se protéger autant à titre personnel que professionnel. En termes de sensibilisation, nous conseillons à nos clients de dire à leurs salariés : ce qu'on vous demande de faire pour protéger le patrimoine de l'entreprise (bonne pratique sur la gestion des mots de passe, l'application des correctifs, etc.) appliquez-le aussi à votre vie personnelle numérique.

Mots clés : cyberattaque, cyberdéfense, cybermenaces, cybersécurité, hackeur, rançongiciels, ransomware, sécurité logicielle

Citation : Jean-Luc Moliner, Marion Videau, Jean-Yves Poichotte, Denis Pélanchon & Nicolas de Rycke. (2022). *La cybersécurité et les entreprises : une vision de terrain*. Les séances thématiques de l'Académie des technologies. @

Académie des technologies. Le Ponant, 19 rue Leblanc, 75015 Paris. 01 53 85 44 44. academie-technologies.fr

Production du comité des travaux. Directeur de la publication : Denis Ranque. Rédacteur en chef de la série : Hélène Louvel. Auteur : Marie-Claude Treglia. N°ISSN : 2826-6196.