TECHNIQUES
DE L'INGÉNIEUR

LES FOCUS
TECHNIQUES DE L'INGÉNIEUR

L'INDUSTRIE
FACE AUX DÉFIS DE LA CYBERSÉCURITÉ

décembre / 2022

SOMMAIRE

INTRODUCTION

L'Agence de l'Union européenne pour la cybersécurité a publié son rapport annuel le 3 novembre 2022 : "ENISA Threat Landscape 2022". Il en ressort une hausse continue des attaques informatiques. Ces menaces gagnent en nombre et en variété. Et leurs cibles se diversifient : l'industrie et les infrastructures critiques s'ajoutent aux entreprises.

L'industrie intègre de plus en plus de composants informatiques pour gagner en efficacité. Cette surface d'attaque augmentée en fait une cible de choix pour les pirates informatiques. L'"OT" - Operational Technology - est au cœur du fonctionnement industriel, de même que l'"IT" déploie et entretient un réseau vital au sein de l'entreprise. A la différence des entreprises, l'industrie est confrontée à une gestion de la sécurité plus complexe, liée à la variété des outils et à l'obligation de continuité de service. Les réseaux "IT" et "OT" encore séparés il y a peu, convergent avec la transition numérique amorcée il y a quelques années. La conséquence est que l'infrastructure industrielle n'échappe plus aux maux de l'informatique.

De leur côté, les éditeurs d'antivirus et les experts en cybersécurité découvrent chaque jour de nouveaux virus et codes malveillants, de plus en plus sophistiqués. Que les pirates tentent d'infiltrer des réseaux informatiques sans être repérés ou de mener des actions très ciblées, leur motivation est bien souvent l'appât du gain.

Les infrastructures critiques (pétrole, gaz…) et les industriels font face à des actions toujours plus nombreuses menées par des cybercriminels, qui agissent parfois pour le compte d'Etats. Leur protection aussi complexe que l'architecture de leur réseau est à la fois un casse-tête et une aubaine pour les pirates.

Ce livre blanc se conclue par un entretien avec Haithem Gardabou, Managing consultant en cyberstratégie chez IBM France Sécurité. Les attaques visant les industries ont augmenté de 2 200 % en 2021, selon l'équipe de cybersécurité X-Force d'IBM. Du fait du contexte géopolitique notamment, ces dernières ciblent de plus en plus les infrastructures nationales critiques. Notre interlocuteur observe que face aux différentes menaces, les industriels adoptent des approches plus matures.

L'INFRASTRUCTURE INDUSTRIELLE GAGNE EN MATURITÉ

LA SÉCURITÉ DES INFRASTRUCTURES INDUSTRIELLES RESTE TROP VULNÉRABLE AUX ATTAQUES

Les industriels sont prévenus : « risque accru pour les réseaux de technologie opérationnelle » avertit l'European Union Agency for Cybersecurity. En intégrant de plus en plus de composants informatiques, les industries sont confrontées aux mêmes menaces que les entreprises. Mais la gestion de leur sécurité est plus complexe. Un contexte favorable aux attaques organisées par des États.

Dans son dernier rapport « Threat Landscape », paru fin novembre dernier, l'agence européenne indique que *« l'intérêt des acteurs étatiques à cibler les infrastructures critiques et les réseaux de technologie opérationnelle augmenterait certainement dans un proche avenir ».*

L'ENISA*[1]* n'est pas la seule à tirer la sonnette d'alarme. Tous les experts en cybersécurité et les agences gouvernementales, comme l'ANSSI en France, constatent de plus en plus de collecte de renseignements et de déploiement de logiciels malveillants ciblant l'OT. L'Operational Technology est en effet un rouage essentiel aux industriels. Il concerne en effet les composants matériels et logiciels qui détectent ou contrôlent les équipements industriels (machines-outils, bras robotisés, robots, chaînes de production…).

Ce maillon essentiel est maintenant dans le viseur des pirates. Publiée l'an passé, une étude mondiale de Fortinet, un des leaders de la cybersécurité, indiquait que 93 % du secteur OT avaient subi une intrusion sur les 12 derniers mois et 78 % en avaient enregistré plus de trois. Aucun secteur n'y échappe : industries pétrolière et gazière, production et distribution d'électricité, l'aviation, la marine, le ferroviaire, etc.

Convergence

Ces risques doivent être pris au sérieux par tous les industriels, car il y a une convergence des réseaux informatiques (IT – Information Technology) et industriels (OT – Operational Technology). Auparavant, les réseaux informatiques IT et OT étaient gérés séparément. Mais depuis quelques années, avec la transformation numérique, la convergence entre ces deux sphères est de plus en plus forte.

Or, l'intégration progressive dans les systèmes OT de fonctionnalités informatiques innovantes est à double tranchant : elle permet de gagner en efficacité, mais elle augmente aussi la surface d'attaque.

En un mot, l'infrastructure industrielle n'échappe plus aux maux de l'informatique : vulnérabilité, gestion des mots de passe, déploiement de correctifs de sécurité… Mais à la différence de la cybersécurité des réseaux informatiques « conventionnels », la cybersécurité industrielle a des contraintes particulières. Pour les industriels, l'un des défis principaux est d'assurer la continuité de service.

S'il est possible de faire redémarrer des ordinateurs pour appliquer une mise à jour majeure, il n'est pas aussi évident d'arrêter et de redémarrer une chaîne de production ou des automates surveillant un réseau ferroviaire. Autre difficulté inhérente à l'OT : il s'agit de systèmes qui ont parfois plusieurs décennies d'existence et sur lesquels plusieurs sociétés de maintenance sont intervenues, mais il n'existe pas forcément d'historique précis des modifications… Impossible d'avoir une vision précise et exhaustive

de l'infrastructure industrielle.

Attaques menées par des États

La situation est d'autant plus inquiétante que les industriels ne sont pas prêts à affronter ces différentes menaces. La preuve, plus d'un tiers (35 %) des entreprises interrogées ne savent pas si leur organisation a été victime d'un piratage selon le rapport SANS « The State of OT/ICS Cybersecurity in 2022 and Beyond ». Le Sans Institute est une organisation regroupant 165 000 professionnels de la sécurité ayant pour but de mutualiser l'information concernant la sécurité des réseaux informatiques.

Ce contexte est donc favorable aux cyberattaquants. Mais pas n'importe lesquels. Si les médias relatent régulièrement des attaques visant une cartonnerie ou un fabricant de porcelaine, ces affaires relèvent de l'anecdote. Sans pour autant minimiser les impacts d'une action malveillante pour l'entreprise et ses salariés (perte d'activité durant plusieurs semaines, trésorerie affectée, impacts psychologiques…), ces affaires montrent que les cibles n'étaient pas prêtes, mais surtout qu'elles n'ont pas eu de chance. Elles ont été victimes d'une attaque de masse.

Ce n'est pas le cas des attaques ciblées. Organisées par des États, elles visent à impacter l'activité d'un pays en paralysant les industries essentielles.

[1] Acronyme de The European Union Agency for Cybersecurity.

01/12/2022

DES VIRUS DE PLUS EN PLUS SOPHISTIQUÉS

Chaque jour, les éditeurs d'antivirus et les experts en cybersécurité découvrent de nouveaux virus (ou de multiples variantes) de plus en plus sophistiqués. Pour les pirates et les groupes à la solde de pays, il s'agit d'infiltrer des réseaux informatiques sans être repérés ou de mener des actions très ciblées.

1983 a vu la création par Fred Cohen – considéré comme l'un des pères de la virologie grâce à ses travaux menés dans les années 1980 lorsqu'il était étudiant à l'université de Californie*[1]* – d'un des premiers virus, lesquels se comptent désormais par milliers.

Aujourd'hui, la diversité des programmes malicieux a obligé les spécialistes à parler de « codes malveillants » (ou malwares) plutôt que de virus. La volonté des pirates a aussi évolué. L'appât du gain est devenu leur principale motivation. Pour mener à bien leur forfait, ils disposent dorénavant d'une palette de programmes malveillants très variée : virus, vers, chevaux de Troie…

Ils diffèrent sur de nombreux points, tels que le vecteur d'infection, la réplication, la distribution, la propagation et le contrôle de l'attaquant. D'un point de vue technique, il est également possible de différencier les composants en fonction de leurs capacités :

- charges utiles : le virus en lui-même ;
- droppers : extraction de fichiers du réseau informatique de l'entreprise ciblée ;
- backdoors : « porte dérobée » dans un logiciel ou un matériel permettant d'accéder au réseau informatique ;
- stealer : cheval de Troie (ou *trojan horse*) qui collecte des informations, principalement de connexion (identifiant, mots de passe) ;
- packers : outil chiffrant, compressant ou modifiant le format d'un code malveillant pour le faire ressembler à un fichier anodin… ;
- wiper : un logiciel malveillant conçu pour endommager le système d'exploitation d'un ordinateur ou d'une machine en détruisant de façon irrévocable tous les fichiers.

Les wipers n'ont pas beaucoup évolué depuis que le virus « Shamoon » avait paralysé quelque 30 000 ordinateurs et serveurs chez Saudi Aramco il y a plus de dix ans. Mais différentes études ont constaté un regain d'intérêt pour ce type de code malveillant dont il existe maintenant une vingtaine de variantes.

Industriels : cibles de certains pays

Cette année, des activistes et les groupes travaillant pour des États ont déployé de très nombreux wipers (appelés notamment WhisperGate et HermeticWiper) durant des cyberattaques. Principale cible, l'Ukraine avant que l'invasion du pays par la Russie commence en février.

Pour que les différents maillons d'un code malveillant restent discrets, le développement des composants requiert des expertises spécifiques et un développement continu pour s'adapter aux évolutions des environnements informatiques des victimes. Ces codes sont vendus, partagés et réaffectés, ce qui complique la tâche des experts en cybersécurité et des forces de l'ordre. Il est donc très difficile d'identifier correctement les acteurs de la menace impliqués dans une campagne de logiciels malveillants.

Les réseaux des industriels n'échappent pas à cette évolution de la menace. En avril dernier, le gouvernement américain a tiré la sonnette d'alarme après avoir découvert de nouveaux outils personnalisés capables de compromettre et de perturber entièrement des systèmes et des serveurs ICS/SCADA (Supervisory Control And Data Acquisition ou Système de contrôle et d'acquisition de données). Grâce aux systèmes SCADA, les organisations peuvent contrôler leurs processus industriels soit sur place, soit à distance, et interagir directement avec les équipements, tels que les moteurs, les pompes et les capteurs.

L'alerte conjointe du département de l'énergie, de la NSA et du FBI portait sur des virus développés précisément pour causer des dommages importants aux automates de Schneider Electric et d'OMRON Corp.

« En compromettant et en maintenant un accès complet au système des dispositifs ICS/SCADA, les acteurs malveillants pourraient élever leurs privilèges, se déplacer dans un environnement industriel et perturber les dispositifs ou fonctions critiques », selon l'avis des services américains.

Une preuve supplémentaire que les industriels sont devenus des cibles prioritaires pour certains États…

[1] University of Southern California's School of Engineering (nom actuel : Viterbi School of Engineering)

05/12/2022

LES RÉSEAUX INDUSTRIELS SONT CONFRONTÉS À DE MULTIPLES ATTAQUES ET… CONTRAINTES

Les infrastructures critiques (pétrole, gaz…) et les industriels sont de plus en plus confrontés à des actions menées par des cybercriminels et des États. Mais leur protection est aussi complexe que l'architecture de leur réseau ! Un casse-tête et une aubaine pour les pirates.

En juin 2016, Saint-Gobain est touché par NotPetya, un ransomware qui profitait d'une faille dans Windows. Lancée par le groupe de pirates Shadow Brokers, cette cyberattaque coûtera environ 250 millions d'euros au géant ! L'opérateur télécom espagnol Telefonica et Renault en seront également victimes.

Trois ans plus tard, Norsk Hydro, un des principaux producteurs d'aluminium au monde, est impacté par une attaque de ransomware. Le groupe avait été contraint de fermer de nombreuses usines afin d'éviter la propagation du logiciel malveillant à l'ensemble de ses sites industriels.

L'année 2021 a été particulièrement dure pour le secteur de l'agroalimentaire français. Lactalis, le producteur de champagne français Laurent-Perrier et le groupe Avril (connu pour ses marques Lesieur, Matines…) auront été victimes du même genre de code malveillant. La même année, l'activité de la filiale américaine du géant brésilien de la viande JBS est bloquée par un code malveillant. L'entreprise aura été contrainte de stopper ses activités aux États-Unis, au Canada et en Australie. Quelque temps plus tard, la société révélera avoir payé une rançon de 11 millions de dollars pour récupérer l'accès à ses données.

Actions de sabotage

Ces quelques exemples confirment qu'aucun secteur industriel n'est épargné et que ces menaces remontent déjà à plusieurs années. Mais la situation est devenue très complexe et risquée pour les industriels.

« Nous trouvons de plus en plus de techniques et d'outils tout prêts avec de la documentation sur internet. D'années en année, on rehausse le niveau des personnes malveillantes qui peuvent attaquer des systèmes de plus en plus complexes », constate Renaud Lifchitz, Directeur Scientifique chez Holiseum, une entreprise française spécialisée dans la cybersécurité des infrastructures critiques et industrielles.

Même si les guerres conventionnelles existent encore, des opérations de cyberguerre visant des réseaux industriels sont également menées par des États. Des sabotages entraînant des coupures massives d'électricité ont ainsi été menés en Ukraine.

Pour les industriels, la situation est très difficile à gérer. Les réseaux deviennent de plus en plus complexes et ils sont connectés entre eux. Or, les interconnexions entre univers IT (Information Technology) et OT (Operational Technology) représentent dorénavant un maillon faible de la sécurité.

Prenons l'exemple d'un ERP (Entreprise Resource Planning). Pour centraliser l'ensemble des outils nécessaires à la gestion d'une entreprise, ce logiciel est donc connecté à la chaîne de production. Une faille de sécurité au niveau de ce programme peut être exploitée par un cybercriminel. En infiltrant tout le réseau informatique, il peut récupérer des données sensibles ou les chiffrer (dans le langage courant, on parle plutôt de crypter) pour exiger une rançon (attaque de type ransomware ou rançongiciel).

Liaisons dangereuses

Outre ces interconnexions dangereuses, il y a une inertie générale, que ce soit au niveau de la mise à jour des systèmes et au niveau de la sécurisation de systèmes eux-mêmes, car *« la priorité des industriels est la disponibilité de leur outil de production au détriment de la confidentialité ou de l'intégrité des données. Ils ne veulent pas que leur activité soit interrompue. Tout arrêt ou transformation/amélioration du système informatique par de nouveaux programmes ou processus est considéré comme une perte d'argent »*, souligne Renaud Lifchitz.

Or, beaucoup de systèmes d'exploitation installés dans les usines sont obsolètes. Il n'est pas rare de voir des ordinateurs fonctionnant sous Windows 95, 98, Millenium et pour lesquels Microsoft n'assure plus aucun support (mises à jour, publication et correctifs de sécurité…) depuis des années !

Autre écueil, les fabricants d'automates ne garantissent un support que si leurs clients laissent en l'état la configuration et, en particulier, le mot de passe par défaut. *« Cette pratique est entièrement assumée par les constructeurs, car ces mots de passe sont utilisés pour l'administration et la maintenance. Dans le contrat de prestation, il est d'ailleurs stipulé que leur modification entraîne la rupture du support »,* précise Renaud Lifchitz.

Dans ce contexte, les industriels doivent mettre en place des procédures adaptées pour limiter les risques d'infection virale. Étant donné qu'il n'est pas possible de modifier la configuration des machines, *« la seule parade est d'isoler physiquement les réseaux et surtout de ne pas les connecter à l'internet ou, si c'est le cas, de passer par des couches fonctionnelles (supervision, management, opérations…) intermédiaires. Une isolation périmétrique du réseau est indispensable afin qu'il n'y ait pas d'attaquant dans le même périmètre »*, explique Renaud Lifchitz.

Pour appliquer ces règles essentielles, il est nécessaire de respecter la norme ISO 62443 qui définit la séparation en couche fonctionnelle dans le réseau industriel. Mais elle n'est pas systématiquement appliquée par les industriels…

06/12/2022

HAITHEM GARDABOU : « EN MATIÈRE DE CYBERSÉCURITÉ, LES INDUSTRIELS SONT EN TRAIN DE RATTRAPER LEUR RETARD »

Les attaques visant les industries ont augmenté de 2 200 % en 2021, selon l'équipe de cybersécurité X-Force d'IBM. Du fait du contexte géopolitique notamment, ces dernières ciblent de plus en plus les infrastructures nationales critiques. Face aux différentes menaces, les industriels adoptent des approches plus matures. Explications avec Haithem Gardabou, Managing consultant en cyberstratégie, IBM France Sécurité.

Après avoir obtenu un diplôme d'ingénieur (Administrateur réseaux et systèmes) à l'Institut National des Sciences Appliquées et de Technologies INSA, Haithem Gardabou a multiplié les certifications : Certified Information Systems Security Professional (CISSP), ISO 27001 Lead Implementer. Il est intervenu comme consultant « Security IT » chez EDF, Bouygues Telecom avant de rejoindre IBM en 2019 où il conseille notamment les Comités de Direction : stratégies, business cases, remontée de risques et plans de mitigations...

Techniques de l'Ingénieur : Pourquoi les réseaux des industriels sont-ils un maillon faible ?

Haithem Gardabou : Auparavant, les réseaux industriels étaient des systèmes et des équipements figés. Ils n'étaient pas changés pendant des années, voire des décennies. Ces équipements étaient dans une sorte de « boîte noire » : ils étaient bien isolés des autres réseaux et seul le personnel des opérations pouvait y accéder. Aujourd'hui, cette convergence entre l'IT (Information Technology) et l'OT (Operational Technology), la connexion des réseaux informatiques (analyse de données, intelligence des données, supervision centralisée…) a ouvert cette « boîte noire », ce qui a augmenté la surface d'attaque des industriels.

Comment ont réagi les industriels ?

Les fabricants d'automates et les industriels sont en train de rattraper leur retard. Nous constatons davantage de maturité chez nos clients, même s'ils ont encore des idées reçues sur leurs systèmes : leur chaîne de production n'est pas connectée à Internet (sous-entendu, les pirates ne pourraient pas accéder à leurs réseaux), leur usine est petite (sous-entendu les attaquants ne vont pas les cibler), leurs solutions industrielles sont très complexes avec des protocoles propriétaires (sous-entendu, les attaquants ne pourraient pas comprendre comment ils fonctionnent).

Mais avec ces idées reçues, les industriels oublient que les attaquants ciblent de petites entités, car elles sont moins bien sécurisées que les grands comptes. Différentes attaques ont démontré que les pirates avaient infiltré les gros industriels par rebond, c'est-à-dire en commençant par infiltrer le réseau de leurs sous-traitants.

Quelle est la position des fabricants d'automates ?

Les principaux fournisseurs publient des guides sur la cybersécurité et incitent leurs clients à suivre leurs recommandations, que ce soit en amont (avant la mise en place d'automates) ou en aval, lors des différentes interventions (notamment lors des maintenances). Mais dans les environnements réglementés comme la santé et la pharmacie, la modification de ces systèmes (par exemple, le changement

du mot de passe par défaut) par les industriels eux-mêmes peut entraîner la perte de différentes certifications et de la garantie de ces machines. Pour répondre au contexte actuel, il convient donc aux fabricants de modifier certains points critiques (mot de passe ou compte par défaut par exemple) ou de recommander de changer les équipements arrivant en fin de vie, car ils seraient considérés comme des matériels défectueux.

Quelles sont les bonnes pratiques à mettre en place ?

S'il existe des équipements avec des protocoles vulnérables et qui engendrent un impact critique, il faut commencer par les isoler physiquement et logiquement. C'est indispensable, mais les dernières attaques ont montré que cet isolement n'était pas correctement réalisé chez toutes les entreprises. Les industriels doivent aussi déployer des solutions plus innovantes et performantes. Une fois déployées sur site, on leur laisse un peu de temps pour que leurs moteurs d'intelligence artificielle et de connaissance maîtrisent précisément l'environnement et les différentes opérations. Une fois le contexte maîtrisé, ces systèmes passent en mode détection. Dès qu'un comportement anormal (un changement de process un samedi soir, une modification de la température enregistrée par un capteur…) est repéré au niveau opérationnel, une alerte est envoyée au système central pour lancer des investigations. La partie cybersécurité de ces solutions va alors scanner tous les équipements et s'appuyer sur une base de connaissance des failles. Dès qu'une tentative d'intrusion exploitant une vulnérabilité a été constatée, elle bloque l'attaque et lève l'alerte au centre des opérations. Cette méthode, proactive et réactive, permet de conserver des solutions vulnérables tout en gardant la maîtrise de l'environnement, car leur changement serait complexe et long. Ce n'est pas comme si on changeait un simple ordinateur portable.

07/12/2022

POUR ALLER PLUS LOIN

L'EUROPE VEUT PROTÉGER SES COMMUNICATIONS SENSIBLES GRÂCE AU QUANTIQUE

Depuis 2019, les 27 États membres de l'UE travaillent au développement d'une infrastructure européenne de communication quantique (EuroQCI). C'est pour répondre à cet objectif que l'agence spatiale européenne (ESA), la Commission européenne et la SES (Société Européenne des Satellites) ont annoncé le développement d'un système de distribution de clés cryptographiques par satellite.

Le nerf de la guerre est l'information. Et en la matière, les amitiés officiellement annoncées par des États restent juste des déclarations diplomatiques. Il y a quelques années, WikiLeaks avait révélé que trois anciens présidents de la République française avaient été espionnés par les Américains. Une station d'écoute avait été installée au dernier étage de l'ambassade américaine à Paris.

Si différentes techniques sont employées par les agences de renseignement pour récupérer des informations sensibles, de nombreux États anticipent aussi de nouvelles parades. C'est le cas de l'Europe avec son initiative EuroQCI lancée en juin 2019. Objectif : construire une infrastructure de communication quantique sécurisée qui couvrira l'ensemble de l'UE, y compris ses territoires d'outre-mer d'ici 2027.

L'EuroQCI protégera les données sensibles et les infrastructures critiques en intégrant des systèmes quantiques dans les infrastructures de communication existantes, fournissant ainsi une couche de sécurité supplémentaire basée sur la physique quantique. Elle renforcera la protection des institutions gouvernementales européennes, de leurs centres de données, des hôpitaux, des réseaux d'énergie, etc.

Communications laser

L'EuroQCI comprendra un segment terrestre reposant sur des réseaux de communication en fibre optique reliant des sites stratégiques au niveau national et transfrontalier, et un segment spatial basé sur des satellites. Il reliera les réseaux nationaux de communication quantique à travers l'UE et assurera une couverture mondiale.

La communication par satellite commence à devenir concrète avec l'annonce par l'agence spatiale européenne (ESA), la Commission européenne et la SES (Société Européenne des Satellites, connue pour ses satellites dédiés à la TV, Astra) du développement d'un système de distribution de clés cryptographiques par satellite.

Le satellite Eagle-1 sera le premier système spatial de distribution de clés quantiques en Europe. Il devra démontrer la faisabilité du système de distribution quantique développé dans le cadre du programme Scylight (Secure and Laser communication technology) de l'ESA.

Les liaisons optiques présentent notamment l'avantage d'éviter les interférences et la détection. Par rapport aux fréquences radio déjà encombrées, la communication laser est extrêmement difficile à intercepter en raison d'un faisceau beaucoup plus étroit. Elles sont également capables de transporter des quantités de données bien plus importantes que les autres solutions.

Pesant environ 300 kg, l'appareil sera construit par la société italienne Sitael, et Tesat fournira les terminaux de communication optique. L'engin spatial fonctionnera sur une orbite héliosynchrone de 500 km, effectuant plusieurs vols par jour au-dessus de stations terrestres européennes, ce

qui sera suffisant pour tester le système.

D’autres projets de satellites quantiques

Pour mettre en œuvre un système d'échange de clés cryptographiques très sécurisé, le consortium chargé d’Eagle-1 développera une charge utile QKD (Quantum Key Distribution), une station optique terrestre, des réseaux d'exploitation quantiques évolutifs et un système de gestion des clés pour interagir avec les infrastructures nationales QCI (Quantum Communications Infrastructure). Le lancement du système est prévu en 2024 pour une mission de trois ans, les tests devant être effectués d'ici 2025.

Le coût du programme, y compris le satellite et les systèmes au sol, est d'environ 130 millions d’euros. Huit pays membres de l'ESA – Allemagne, Autriche, Belgique, Italie, Luxembourg, Pays-Bas, République tchèque et Suisse – contribueront au projet, avec le soutien de la Commission européenne.

L’Europe n’est pas la seule à tester ce type d’infrastructure. En 2016, la Chine avait lancé un satellite appelé Micius, présenté par les médias d'État chinois comme le premier satellite quantique au monde.

D’autres projets sont également annoncés. La start-up singapourienne SpeQtral prévoit de déployer son premier satellite quantique en orbite basse en 2024. En septembre dernier, elle a signé un accord pour utiliser les services au sol de Thales Alenia Space. Parallèlement, Virgin Orbit devrait lancer l’année prochaine les premiers satellites LEO pour la société britannique Arqit, spécialisée dans le cryptage des technologies quantiques.

07/11/2022

LES RÉSEAUX 5G PRIVÉS : L'ÉPINE DORSALE DE L'INDUSTRIE 4.0 ?

Cette nouvelle génération permet aux industriels de s'appuyer sur l'automatisation pour disposer de systèmes de production moins énergivores. Afin de bénéficier d'un confort d'utilisation plus important, des industries commencent à déployer leurs propres réseaux 5G.

Avec la 5G, les entreprises bénéficient d'un débit multiplié par 20. La latence, autrement dit la durée de voyage d'une data entre son émission et sa réception, est également divisée par 10 (voire 20). Le nombre de terminaux qu'une antenne peut gérer convenablement est multiplié par 100 !

La 5G permet donc d'améliorer la fiabilité des processus industriels. Mais pour gagner en efficacité tout en renforçant la sécurité des connexions, des industriels européens décident de gérer eux-mêmes leur propre réseau.

Selon GlobalData|1], l'Europe est à la pointe de la 5G et des réseaux privés, et la région a commencé à s'imposer dans les déploiements de l'industrie 4.0. Le Connected Enterprise Tracker, récemment proposé par cette société a révélé que le secteur manufacturier représente près d'un tiers des déploiements de la 5G et des réseaux privés, et une grande partie de cette activité est concentrée en Europe (56 % des déploiements jusqu'à présent).

Les industriels qui pilotent des machines automatisées génèrent une grande quantité de données qui doivent être transférées, analysées et surveillées en temps réel. Cela nécessite des réseaux de transmission sans fil à faible latence et hautement sécurisés.

La 5G privée répond à toutes ces exigences, mieux que ses prédécesseurs comme le Wi-Fi, la 4G-LTE ou les connexions filaires. La connectivité basée sur l'Ethernet filaire est très bon marché et offre une qualité de communication et des performances stables. Toutefois, comme elle est câblée, elle ne peut pas assurer la mobilité. Le coût du câblage est élevé et le temps de construction est trop long.

Les dispositifs basés sur le Wi-Fi sont faciles à déployer dans l'usine, où le coût de déploiement du réseau est faible, mais ils présentent toujours des inconvénients : les connexions de communication sans fil sont instables, la distance de communication est courte, la latence est supérieure à quelques dizaines de millisecondes et elles sont vulnérables aux menaces extérieures.

Or, qu'il s'agisse de maintenance préventive ou d'arrêts de sécurité, tout retard peut causer de nombreux dommages. Les données doivent également être protégées des cyberattaques.

Accéder rapidement aux données

Le déploiement de réseaux 5G privés va s'accélérer au fur et à mesure que les entreprises migrent une partie de leurs données dans l'edge computing. Cette « informatique de périphérie » est un cadre informatique distribué qui déplace les ressources informatiques stockées dans le cloud et dans les datacenters aussi près que possible de la source d'origine. Son adoption permettra ainsi d'accéder aux données essentielles plus rapidement et d'écarter celles qui ne sont plus nécessaires, ou de les stocker dans le cloud.

La combinaison de la 5G privée avec l'edge computing devrait favoriser l'automatisation de la maintenance et les fonctions de base des machines, ce qui réduira la quantité d'interactions et d'efforts nécessaires aux humains. Différentes activités industrielles devraient donc bénéficier des atouts des réseaux 5G privés.

Par exemple, les opérations pétrolières et gazières produisent un volume très important de données qui doivent être récupérées et stockées efficacement. De nombreuses entreprises de ce secteur annoncent notamment des inves-

tissements dans des technologies d'efficacité énergétique comme la 5G privée.

Les installations minières nécessitent quant à elles qu'une zone massive soit couverte. Or, les technologies sans fil conventionnelles comme le Wi-Fi et la 4G LTE s'avèrent incompatibles en raison d'une communication limitée et à faible portée. Avec la 5G privée, elles devraient pouvoir automatiser de nombreuses opérations sur site.

[1] GlobalData Plc est une société de conseil qui fournit des plateformes de données et d'analyse

11/10/2022

ATTAQUES INFORMATIQUES : LE HARDWARE DEVIENT UNE CIBLE

Tout dispositif matériel comporte un micrologiciel, un vecteur d'attaque tentant pour de nombreux pirates. L'industrie a progressé en matière de solutions de sécurité des microprogrammes. Mais la prolifération de l'Internet des objets et des systèmes embarqués dans les voitures inquiète les experts en sécurité informatique.

Régulièrement, la presse se fait l'écho d'applications mobiles qui récupèrent vos données personnelles à votre insu. Mais il existe une menace encore plus forte, mais qui reste très discrète : le piratage de composants électroniques intégrés dans les téléphones.

Une récente étude menée par des chercheurs de l'Université de Pittsburgh Swanson School of Engineering a révélé que le circuit spécialisé dans la génération d'images (GPU-Graphics Processing Unit) de certains smartphones Android, intégrant une puce Qualcomm Adreno, pouvait être utilisé pour espionner et récupérer des données personnelles.

Présentée en mars 2022 lors de la conférence ASPLOS en Suisse, une attaque reposant sur cette faille de sécurité matérielle permet de déduire différentes données d'identification (dont les logins et mots de passe) sans nécessiter de privilège système ni provoquer de changement notable dans le fonctionnement ou les performances de l'appareil. Le pire est que ce piratage passe inaperçu ! Google a confirmé qu'il publierait une mise à jour de sécurité Android dans le courant de l'année pour résoudre ce problème.

Effet domino

Les attaques visant le hardware ont d'abord été imaginées pour *« le vol de données bancaires sur les puces de nos cartes bleues,* détaille dans le journal du CNRS Lilian Bossuet, professeur à l'université Jean Monnet de Saint-Étienne et membre du laboratoire Hubert Curien. *Ces approches sont à présent appliquées aux téléphones portables, dont les circuits sont mal protégés. La situation est cependant encore pire dans l'Internet des objets, où les appareils sont à la fois omniprésents et très peu, voire pas du tout, sécurisés. »*

Ordinateurs, réseaux de communication, capteurs… Tous les appareils électroniques intégrant des processeurs. Il suffit qu'un composant physique soit compromis pour impacter les différentes couches de cybersécurité d'un système. L'effet serait dévastateur. Or, les puces modernes sont des dispositifs très complexes constitués de milliards de transistors. Leur compromission peut se faire à différentes étapes (conception, fabrication, assemblage, test), mais par contre la détection est très difficile.

Les modifications physiques apportées à un seul circuit intégré peuvent être bien cachées parmi le nombre de composants valides et peuvent fonctionner longtemps sans être détectées. Une vulnérabilité matérielle bien conçue peut donc passer inaperçue !

À l'occasion de la conférence Black Hat sur la sécurité à Las Vegas, en 2012, le chercheur Jonathan Brossard avait créé une backdoor baptisée Rakshasa qui remplace le Bios d'un ordinateur. Son programme malveillant pouvait compromettre le système d'exploitation au moment du démarrage sans laisser de traces sur le disque dur. Jonathan Brossard avait ainsi démontré que le backdooring permanent du matériel était possible.

Espionnage économique

La situation est d'autant plus inquiétante que les attaques matérielles concernent de multiples dispositifs : systèmes de contrôle d'accès, appareils de réseau, systèmes de contrôle industriel, systèmes de surveillance…

Outre l'intégration de portes dérobées (ou backdoor), ces attaques peuvent être utilisées pour de l'écoute clandestine, la génération d'erreurs entraînant l'arrêt d'une machine, le contournement des systèmes d'authentification informatique…

Autant de techniques mises à profit pour de l'espionnage économique ou perturber le bon fonctionnement d'industriels sensibles. Fin 2018, des usines chinoises avaient implanté des puces de surveillance et de contrôle du réseau sur des cartes mères fabriquées pour Supermicro. Quelques années plus tôt, des défaillances surprenantes de composants avaient été détectées chez des entreprises de défense telles que Raytheon, BAE, Northrop Grumman et Lockheed.

Le risque d'acquérir des composants matériels avec une porte dérobée est donc une réalité. Mais les Chinois ne sont pas les seuls à exploiter cette technique. La NSA a aussi demandé aux fabricants américains d'implanter une porte dérobée dans les produits exportés.

Mais comment se protéger face à toutes ces menaces ? *« Pour des questions de performances, de nombreux processeurs partagent des zones de mémoire cache, où ils peuvent laisser des informations qui deviennent alors vulnérables. Il faut réfléchir à de nouvelles architectures qui permettent d'isoler physiquement les informations critiques. Mais renforcer la sécurité a forcément un coût. S'il est accepté pour des applications bancaires ou militaires, il sera plus difficile à tolérer pour des usages conventionnels ou domestiques »*, a prévenu Lilian Bossuet, dans le journal du CNRS.

14/04/2022

INGÉNIEURS : QUELS SONT LES SECTEURS LES PLUS CRÉATEURS D'EMPLOIS ?

Dans les années qui viennent, certains secteurs industriels vont avoir besoin d'ingénieurs : c'est particulièrement le cas dans le secteur informatique au sens large, mais aussi pour les énergies renouvelables.

Le secteur informatique, s'il est aujourd'hui en forte tension, restera dans les années qui viennent un secteur porteur, attractif, et capable d'attirer bon nombre de talents. Selon la récente étude de la Dares, le métier d'ingénieur informatique est d'ailleurs celui qui devrait connaître la plus forte expansion en France d'ici à 2030, avec plus de 115 000 postes créés. Et une augmentation des effectifs de 26%.

Les métiers de l'informatique touchent aujourd'hui également aux activités numériques, à l'intelligence artificielle, au cloud computing… Des sujets que les entreprises investissent en masse, et qui devraient également apporter leur lot en termes de création d'emplois. Emplois qui devraient être pour une grande part être dévolus à des jeunes voire des juniors. En effet, ces derniers devraient, selon un rapport de France Stratégie, les jeunes diplômés combleront, d'ici à 2030, près de trois quarts des besoins en recrutement. Une réalité qui va obliger le secteur à s'adapter, surtout en termes de formation.

Le secteur, également très porteur, de la robotique sera de ceux qui recrutent dans les prochaines années. De même pour l'ingénierie biomédicale. Ces deux secteurs, où la France est compétitive, sont très porteurs pour l'avenir. La robotique, qui va permettre de révolutionner le fonctionnement des usines, et l'ingénierie biomédicale, qui développe de plus en plus d'appareils connectés pour la médecine à distance, vont ainsi nécessiter le recrutement de nombreux ingénieurs.

Les années qui viennent vont aussi voir un secteur avec un besoin en ingénierie important : celui des énergies renouvelables. Avec une transition énergétique plus urgente que jamais et la nécessité de développer des modèles productifs décarbonés, que ce soit pour l'énergie ou pour l'industrie, les ingénieurs en production d'énergie sont très recherchés. Ils vont même peut-être venir à manquer, tout comme les ingénieurs R et D sur ce secteur.

Toujours dans le domaine énergétique, les industries minières et pétrolières vont également avoir des besoins accrus en termes d'ingénieurs. Même si la tendance veut que ces énergies soient de moins en moins consommées, la transition énergétique va prendre du temps. Ainsi, les énergies fossiles continuent à avoir besoin de nouveaux ingénieurs, c'est particulièrement le cas en ce qui concerne l'industrie du gaz.

L'extraction de matériaux rares, de plus en plus importants pour certaines industries, va également entraîner le recrutement de nombreux ingénieurs en R et D et en production, notamment pour mettre en place une exploitation minière plus respectueuse de l'environnement.

Enfin, le secteur de la sécurité informatique, la cybersécurité, va lui aussi être appelé à croître régulièrement durant les prochaines années, alors que les attaques informatiques n'ont jamais été aussi nombreuses contre les entreprises. Ces dernières font émerger deux dangers qui obligent les entreprises à s'armer en conséquence : le vol de données contre rançon, et la mise en péril de l'architecture informatique des entreprises. Les ingénieurs en sécurité informatique sont d'ores et déjà très demandés, et les besoins risquent rapidement de dépasser les ressources.

A côté des secteurs dynamiques, il faut garder à l'esprit les difficultés actuelles de l'industrie en France. Certains secteurs peinent à recruter, pas uniquement à des postes d'ingénieurs bien sûr, mais on estime qu'il y a actuellement quelque 70 000 postes à pourvoir au sein des entreprises industrielles françaises. De nombreux postes d'ingénieurs mais aussi de consultants restent vacants, car les recruteurs ne parviennent plus à dénicher de talents.

27/09/2022

LES FAILLES DE CYBERSÉCURITÉ DITES « 0-DAY » NE CONNAISSENT PAS LA CRISE

La plupart des attaques sont le fruit de codes malveillants « classiques » diffusés par email. Sensibilisés aux menaces numériques, les salariés peuvent en repérer certaines. D'autres peuvent être bloqués par les antivirus. Mais certaines cyberattaques reposent sur des failles dites « 0-day » qui sont par définition plus difficiles à repérer. Résultat, ces vulnérabilités font l'objet de surenchères.

Il y a un mois, l'Assistance Publique – Hôpitaux de Paris (AP-HP) annonçait avoir porté plainte après avoir constaté un vol de fichiers concernant des données sensibles de 1,4 million de personnes testées mi-mai 2020. Ces informations avaient été mises en ligne sur un site de téléchargement basé en Nouvelle-Zélande.

Un mois plus tard, les services de la BL2C (Brigade de lutte contre la cybercriminalité) ont interpellé un étudiant en informatique de 22 ans. Originaire du Var, il a justifié son action en expliquant qu'il souhaitait mettre en lumière les défaillances de sécurité du système informatique de santé, selon France Info.

Une faille pas repérée par les antivirus

Pour infiltrer le réseau d'AP-HP et récupérer cette base de données, cet étudiant a profité d'une faille dite « 0-day » dans un logiciel commercialisé par la société Hitachi Vantara. Ce type d'attaque consiste à exploiter une vulnérabilité dans un logiciel ou un automate avant qu'un correctif ne soit disponible ou largement déployé par l'éditeur de ce programme ou le fabricant de la machine.

Ces attaques peuvent être particulièrement dommageables, car les stratégies de cyberdéfense traditionnelles (comme les antivirus) sont inefficaces pour s'en protéger. Résultat, leur nombre ne cesse d'augmenter. Rappelons que la principale méthode de détection des antivirus repose sur leur base de signatures virales (l'autre solution étant l'analyse comportementale qui n'est pas toujours bien maîtrisée) qui ne peut pas être exhaustive et intégrer des virus ou des failles inconnus.

En permettant d'infiltrer un réseau informatique ou d'accéder au contenu d'un smartphone sans être repéré, les failles « 0-Day » font l'objet de surenchères. Tout le monde se les arrache et en particulier les grandes agences de renseignement du monde entier. Les « 0-day » impactent tous les systèmes d'exploitation, dont Windows, mais aussi les navigateurs et les OS mobiles. Selon différentes bases de données telles que « 0-day tracking project », près de 60 « 0-day » ont été découverts cette année, soit près du double du total par rapport à l'an passé.

2 500 000 dollars pour une faille « 0-day » !

Un vrai business avec des tarifs qui atteignent des sommets. Ceux proposés par exemple par l'entreprise Zerodium montrent une augmentation de 1 150 % des prix au cours des trois dernières années.

Se présentant comme un broker de failles critiques, Zerodium verse de grosses primes aux chercheurs en sécurité afin d'acquérir leurs « 0-day ». *« Alors que la majorité des programmes de bug bounty existants acceptent presque tous les types de vulnérabilités et de PoCs, mais ne paient que très peu, chez Zerodium nous nous concentrons sur les vulnérabilités à haut risque avec des exploits entièrement fonctionnels et nous payons les récompenses les plus élevées du marché (jusqu'à 2 500 000 dollars par soumission) »*, affirme l'entreprise qui a reçu plus de 10 000 soumissions de la part de 1 500 experts en cybersécurité. Zerodium est né des cendres de Vupen Security, une entreprise montpelliéraine créée par de talentueux experts français partis s'exiler aux États-Unis.

13/10/2021

CYBERSCORE : DES CODES COULEURS POUR CONNAÎTRE LE NIVEAU DE SÉCURITÉ DES SITES

En cours de discussion, une proposition de loi souhaite la mise en place d'une certification de cybersécurité des plateformes numériques destinées au grand public. Elle pourrait entrer en vigueur en 2023.

Approuvée le 30 novembre par les députés, cette proposition se présente comme l'équivalent du NutriScore. Retenu dans différents pays, ce système d'étiquetage nutritionnel à cinq niveaux est établi en fonction de la valeur nutritionnelle d'un produit alimentaire.

Présentée fin 2020 par le sénateur Laurent Lafon (UDI), cette proposition de loi pourrait donc déboucher sur l'apparition d'un CyberScore… le 1er octobre 2023. Il concernera les plateformes opérant sur le territoire et « dont l'activité dépasse un ou plusieurs seuils qui seront fixés par décret », donc des réseaux sociaux comme Facebook et Twitter.

Le grand public saura immédiatement si un site a mis en place différents processus de sécurité informatique afin d'assurer la protection des données et notamment celles à caractère personnel.

Pas une usine à gaz

À l'instar du NutriScore, l'affichage du résultat devra être présenté *« de façon lisible, claire et compréhensible et accompagné d'une présentation ou d'une expression complémentaire, au moyen d'un système d'information coloriel »*.

Pour l'instant, ce projet de loi ne détaille pas les critères d'évaluation pour établir le CyberScore (sous forme de certification) d'un site. Mené par des prestataires approuvés (liste pas encore connue) par l'Anssi (Agence nationale de la sécurité des systèmes d'information), l'audit portera évidemment sur la sécurité des données, leur localisation (dont le lieu du ou des datacenters…).

« L'objectif n'est pas de créer une usine à gaz ou un diagnostic long à monter, mais d'identifier quatre ou cinq critères qui permettent assez facilement d'identifier le risque encouru. Il va falloir jauger où on met le curseur avec un double objectif : la fiabilité et le pragmatisme », a précisé Laurent Lafon au site nextinpact.com.

« Comme le Digital Services Act et Digital Markets Act, l'objectif du CyberScore est d'inciter les grandes plateformes à plus de transparence. Comme pour le NutriScore qui indique quand un pain au chocolat industriel est trop gras, ce classement pour la sécurité des données sensibilisera peut-être le grand public, mais aussi tous les professionnels aux risques qu'ils encourent. Tous ceux qui sont tenus au secret professionnel et qui utilisent Whatsapp ou Messenger pour échanger des informations sensibles ou à caractère personnel seront peut-être plus attentifs. Mais comme pour les campagnes qui informent sur les dangers de la cigarette, la prise de conscience et les changements d'habitude prendront du temps », explique Maître Christiane Féral-Schuhl, avocate spécialisée en droit des nouvelles technologies et en droit de la propriété intellectuelle.

Amende peu dissuasive

Le CyberScore entrant dans le champ d'application de l'article L.131-4 du code de la consommation, ce texte de loi prévoit une amende – prononcée par la DGCCRF (Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes) – pouvant aller jusqu'à 375 000 euros.

Un montant qui apparaît comme dérisoire comparé aux

chiffres d'affaires des GAFAM qui ont fortement progressé entre 2019 et 2020 : 182 milliards de dollars pour Alphabet (maison mère de Google) en 2020, 153 milliards pour Microsoft et 77 milliards pour Meta (ex-Facebook).

« La proposition de loi peut encore évoluer et, sur le principe, elle n'est pas choquante. Reste à préciser les modalités et le montant des sanctions, car 375 000 euros ce n'est pas très dissuasif pour les grands acteurs du numérique qui sont ciblés », reconnaît Maître Christiane Féral-Schuhl.

06/12/2021

L'EUROPE VEUT PLUS DE SÉCURITÉ DANS LES OBJETS CONNECTÉS

L'Union européenne travaille sur une proposition de loi dans le cadre du Cyber Resilience Act. L'objectif est d'établir des normes de cybersécurité et des procédures d'évaluation de conformité plus strictes pour les objets connectés grand public, mais surtout industriels.

Téléviseurs, montres, réfrigérateurs, machines à café… De plus en plus d'appareils domestiques sont dits « connectés ». De nombreux secteurs industriels intègrent aussi ces capteurs connectés pour obtenir en temps réels différentes mesures ou pour optimiser la maintenance de machines et d'automates.

Or, l'intégration de ces appareils a un impact sur la vie privée des consommateurs. Quelles données sont récupérées par ces appareils et sont-elles sauvegardées de façon sécurisée ? Pour les industriels, le déploiement de ces capteurs augmente ce que les experts en cybersécurité appellent la « surface d'attaque ». En clair, plus il y a de logiciels, d'ordinateurs, d'automates et d'objets connectés et plus il y a de potentielles tentatives d'intrusion malveillante dans les réseaux et donc d'exfiltration de données.

Cette semaine, la Commission européenne a sifflé la fin de la récré, car depuis des années, les experts tiraient la sonnette d'alarme : trop d'appareils connectés n'intègrent aucune sécurité des connexions et trop d'éditeurs ne mettent pas en place un niveau de sécurité adapté.

Des autorités de surveillance et des amendes

La Commission a donc présenté sa proposition de loi sur la cyber-résilience, qui vise à protéger les consommateurs et les entreprises contre les produits connectés numériquement dont les caractéristiques de cybersécurité sont insuffisantes. La législation sera obligatoire pour tous les États membres de l'UE. Mais elle aura probablement aussi des répercussions à l'échelle mondiale puisque toute entreprise vendant des produits dans l'UE devra s'y conformer.

La loi a été annoncée en septembre 2021 et s'appuie sur la stratégie de cybersécurité de l'UE de 2020. L'objectif est de faire en sorte que les produits numériques, souvent regroupés sous l'appellation « Internet des objets », soient plus sûrs pour les personnes qui vivent et travaillent dans l'Union européenne, et d'accroître la responsabilité des fabricants en matière de respect des exigences minimales.

Selon une fiche d'information publiée par la Commission européenne, 90 % des produits seront autoévalués par les fabricants. Environ 10 % des produits feront l'objet d'une évaluation par un tiers, en raison de leur caractère critique (interfaces réseau, pare-feu, processeurs, etc.).

Les États membres désigneront des autorités de surveillance du marché qui seront chargées de faire respecter les obligations de la loi sur la cyber-résilience. En cas de non-conformité, ces autorités pourront demander aux opérateurs de mettre fin à la non-conformité et d'éliminer le risque, d'interdire ou de restreindre la mise à disposition d'un produit sur le marché, ou d'ordonner le retrait ou le rappel du produit.

L'IoT, nouvelle cible des pirates

Chacune de ces autorités sera en mesure d'infliger des amendes aux entreprises qui ne respectent pas les règles. La loi sur la cyber-résilience établit des niveaux maximums pour les amendes administratives qui devraient être prévues dans les lois nationales en cas de non-conformité.

Il y a urgence, car les réseaux des entreprises et des industriels ressemblent à des gruyères. Reconnaissons que la tâche n'est pas simple pour les équipes chargées de la sécurité informatique de leur entreprise : comment gérer et surveiller précisément un réseau informatique qui ne cesse

de grossir, comme un mille-feuille auquel on ne cesse d'ajouter des couches ?

Les cyberattaquants disposent avec l'IoT d'une porte d'entrée idéale pour s'y infiltrer, disséminer des ransomwares, voler des données ou bien encore lancer des opérations de minage clandestines (cryptojacking). Mais la situation est-elle encore sous contrôle quand 69 % des décideurs informatiques interrogés en France déclarent que leur organisation a constaté une augmentation du nombre d'appareils IoT connectés au réseau d'entreprise en 2020 selon « The Connected Enterprise : IoT Security Report 2021 » de Palo Alto Network, un des poids lourds mondiaux de la cybersécurité.

Preuve que la situation devient explosive, un récent rapport de Nozomi Networks – une entreprise américaine spécialisée dans la protection des réseaux industriels – affirme que les cybercriminels exploitent les capteurs industriels pour lancer des attaques. Selon ce spécialiste, *« l'activité des botnets IoT s'est intensifiée au premier semestre 2022 »*.

À l'instar de ce qui se passe avec l'informatique où des pirates prennent le contrôle d'ordinateurs (des botnets ou « réseaux zombie »), la finalité des capteurs industriels est également détournée par des cybercriminels pour lancer des attaques DDoS (Distributed Denial of Service, déni de service distribué). Le but est de paralyser l'activité d'un serveur ou d'une ressource web en le submergeant de requêtes.

Comme pour les entreprises, les industriels doivent renforcer leur niveau de sécurité afin d'assurer leur pérennité en appliquant des mesures simples, mais efficaces : mots de passe durcis, segmentation des réseaux, contrôle des accès.

19/09/2022

TECHNIQUES
DE L'INGÉNIEUR

Gagnez du temps et sécurisez vos projets en utilisant une source actualisée et fiable

RÉDIGÉE ET VALIDÉE PAR DES EXPERTS

MISE À JOUR PERMANENTE

100 % COMPATIBLE SUR TOUS SUPPORTS NUMÉRIQUES

SERVICES INCLUS DANS CHAQUE OFFRE

- + de 340 000 utilisateurs chaque mois
- + de 10 000 articles de référence et fiches pratiques
- Des Quiz interactifs pour valider la compréhension

SERVICES ET OUTILS PRATIQUES

Questions aux experts*
Les meilleurs experts techniques et scientifiques vous répondent

Articles Découverte
La possibilité de consulter des articles en dehors de votre offre

Dictionnaire technique multilingue
45 000 termes en français, anglais, espagnol et allemand

Archives
Technologies anciennes et versions antérieures des articles

Info parution
Recevez par email toutes les nouveautés de vos ressources documentaires

*Questions aux experts est un service réservé aux entreprises, non proposé dans les offres écoles, universités ou pour tout autre organisme de formation.

Les offres Techniques de l'Ingénieur

INNOVATION
- Éco-conception et innovation responsable
- Nanosciences et nanotechnologies
- Innovations technologiques
- Management et ingénierie de l'innovation
- Smart city – Ville intelligente

MATÉRIAUX
- Bois et papiers
- Verres et céramiques
- Textiles
- Corrosion – Vieillissement
- Études et propriétés des métaux
- Mise en forme des métaux et fonderie
- Matériaux fonctionnels. Matériaux biosourcés
- Traitements des métaux
- Élaboration et recyclage des métaux
- Plastiques et composites

MÉCANIQUE
- Frottement, usure et lubrification
- Fonctions et composants mécaniques
- Travail des matériaux – Assemblage
- Machines hydrauliques, aérodynamiques et thermiques
- Fabrication additive – Impression 3D

ENVIRONNEMENT – SÉCURITÉ
- Sécurité et gestion des risques
- Environnement
- Génie écologique
- Technologies de l'eau
- Bruit et vibrations
- Métier : Responsable risque chimique
- Métier : Responsable environnement

ÉNERGIES
- Hydrogène
- Ressources énergétiques et stockage
- Froid industriel
- Physique énergétique
- Thermique industrielle
- Génie nucléaire
- Conversion de l'énergie électrique
- Réseaux électriques et applications

GÉNIE INDUSTRIEL
- Industrie du futur
- Management industriel
- Conception et production
- Logistique
- Métier : Responsable qualité
- Emballages
- Maintenance
- Traçabilité
- Métier : Responsable bureau d'étude / conception

ÉLECTRONIQUE – PHOTONIQUE
- Électronique
- Technologies radars et applications
- Optique – Photonique

TECHNOLOGIES DE L'INFORMATION
- Sécurité des systèmes d'information
- Réseaux Télécommunications
- Le traitement du signal et ses applications
- Technologies logicielles – Architectures des systèmes
- Sécurité des systèmes d'information

AUTOMATIQUE – ROBOTIQUE
- Automatique et ingénierie système
- Robotique

INGÉNIERIE DES TRANSPORTS
- Véhicule et mobilité du futur
- Systèmes aéronautiques et spatiaux
- Systèmes ferroviaires
- Transport fluvial et maritime

MESURES – ANALYSES
- Instrumentation et méthodes de mesure
- Mesures et tests électroniques
- Mesures mécaniques et dimensionnelles
- Qualité et sécurité au laboratoire
- Mesures physiques
- Techniques d'analyse
- Contrôle non destructif

PROCÉDÉS CHIMIE – BIO – AGRO
- Formulation
- Bioprocédés et bioproductions
- Chimie verte
- Opérations unitaires. Génie de la réaction chimique
- Agroalimentaire

SCIENCES FONDAMENTALES
- Mathématiques
- Physique Chimie
- Constantes physico-chimiques
- Caractérisation et propriétés de la matière

BIOMÉDICAL – PHARMA
- Technologies biomédicales
- Médicaments et produits pharmaceutiques

CONSTRUCTION ET TRAVAUX PUBLICS
- Droit et organisation générale de la construction
- La construction responsable
- Les superstructures du bâtiment
- Le second œuvre et l'équipement du bâtiment
- Vieillissement, pathologies et réhabilitation du bâtiment
- Travaux publics et infrastructures
- Mécanique des sols et géotechnique
- Préparer la construction
- L'enveloppe du bâtiment
- Le second œuvre et les lots techniques

www.techniques-ingenieur.fr

CONTACT : Tél. : + 33 (0)1 53 35 20 20 - Fax : +33 (0)1 53 26 79 18 - E-mail : infos.clients@teching.com

TECHNIQUES DE L'INGÉNIEUR

BON DE COMMANDE

TECHNIQUES DE L'INGÉNIEUR
RESSOURCES DOCUMENTAIRES
Pleyad 1 - 39, bd Ornano - 93200 Saint-Denis
+33 (0)1 53 35 20 20

S.A.S. au capital de 1.375.000 Euros
RCS Paris B 380 985 937 - SIRET 380 985 937 000 24
NAF 5814Z - TVA FR 33 380 985 937

OFFRE

Sécurité des systèmes d'information

Votre atout sécurité pour garantir l'intégrité de vos systèmes
Ref : TIP440WEB

PRÉSENTATION

Des méthodes pour **mettre en place une politique de sécurité** en entreprise,
Des outils pour **identifier et contrôler les différents types d'intrusions**, et pour **prévenir les attaques**,
Des informations pratiques **pour garantir l'intégrité des données en transit**, **sécuriser les accès Internet**,
Les dernières évaluations en matière de **services mobiles et d'authentification des utilisateurs et des machines.**

VOTRE COMMANDE :

Référence	Titre de l'ouvrage	Prix unitaire H.T	Qté	Prix total H.T
TIP440WEB	Sécurité des systèmes d'information	**1 045 €**	1	**1 045 €**
		Total H.T en €		**1 045 €**
		T.V.A : 5,5%		**57,48 €**
		Total TTC en €		**1 102,48 €**

VOS COORDONNÉES :

Civilité ☐ M. ☐ Mme
Prénom
Nom
Fonction
E-mail
Raison sociale
Adresse
Code postal
Ville
Pays

Date :

Signature et cachet obligatoire

UTM /72/WO/WCE5001