GFA CONSULTING GROUP

BULLETIN D'INFORMATION 02 | 2020

AMÉLIORER LA CYBER-RÉSISTANCE DANS LES PAYS DU PARTENARIAT ORIENTAL

ÉDITORIAL

Ces derniers mois, la pandémie de Covid-19 et ses implications mondiales ont représenté de sérieux défis pour les gouvernements, les entreprises et les particuliers. Les projets de GFA dans le monde entier ne sont pas à l'abri de cette situation sans précédent. Nos équipes de projet doivent réagir rapidement et répondre à des besoins aigus. Nombre de nos lecteurs auront connu des difficultés similaires.

Le projet que nous avons récemment lancé et que nous présentons dans cette newsletter, CybersecurityEast, est également concerné. Ses objectifs restent pertinents alors que l'assaut de la pandémie a nécessité de répondre d'abord aux besoins urgents, puis d'adapter les activités et les stratégies au nouveau contexte. Actuellement, nous approchons d'une phase dans laquelle nos consultants - outre les besoins techniques - seront chargés d'offrir des conseils conceptuels sur la manière d'aborder les implications et les effets de la crise de coronavirus dans leur secteur spécifique. Dans ce contexte, nous considérons que nos travaux sur la cyber-résistance sont pertinents pour la situation actuelle. Il est nécessaire de trouver des solutions numériques fiables et sûres dans de nombreux domaines de la vie quotidienne, des vidéoconférences à l'échange électronique et au partage de quantités accrues de données. Cette observation souligne l'importance d'un cyber espace sûr. Les cybercriminels, par exemple, tentent déjà de tirer parti de la dépendance accrue de la société à l'égard de l'espace numérique par des cyberattaques et des crimes liés au corona, tels que le phishing, les attaques de logiciels malveillants, les enregistrements de pages d'accueil malveillantes ou les publicités frauduleuses. Au vu de toutes les nouvelles alarmantes concernant la pandémie, GFA souhaite que tout le monde reste en bonne santé, corps et âme, et qu'il traverse la crise de la coronavirus indemne.

Anja Desai,
Directrice générale, GFA Consulting Group GmbH

Le verrouillage de coronavirus a pris le projet CybersécuritéEst dans sa phase de lancement. Les activités connexes, lancées par GFA plus tôt cette année, ont dû être ajustées. Deux des évaluations de base requises pour les six pays du partenariat oriental (EaP) ainsi que l'événement de lancement du projet et l'atelier régional prévus en mai ont été reportés à septembre. Actuellement, GFA développe des solutions innovantes pour réagir à la situation et soutenir les efforts des pays bénéficiaires pour faire face à la pandémie.

Dans le monde d'aujourd'hui, de plus en plus interconnecté, les cyberattaques sont un phénomène courant et peuvent menacer les gouvernements, les entreprises et les citoyens avec des effets de grande envergure et potentiellement dévastateurs. Ces incidents vont du piratage de comptes de médias sociaux et du vol d'informations de sécurité sociale aux attaques contre les systèmes financiers et les infrastructures critiques.

Les cyberattaques ne se contentent pas d'augmenter en nombre, elles deviennent aussi de plus en plus sophistiquées. La cybersécurité désigne donc l'ensemble des technologies, processus et pratiques conçus pour protéger les réseaux, les dispositifs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés.

CYBERSECURITYEAST EN BREF

En 2013, l'Union européenne (UE) a adopté sa première stratégie globale relative au cyberespace. L'UE a explicitement reconnu la nécessité de favoriser les initiatives de développement des capacités dans ce domaine. Depuis lors, plusieurs initiatives et projets de développement des capacités liées au cyberespace ont été lancés.

En novembre 2019, le département Gouvernance de GFA a remporté le contrat de service pour CybersecurityEast, le premier projet axé sur le renforcement de la cyber-résistance jamais soumis à un appel d'offres dans le cadre d'une procédure ouverte. Le projet se déroulera jusqu'en novembre 2022 et vise à renforcer les pays du partenariat oriental (Arménie, Azerbaïdjan, Belarus, Géorgie, Moldavie et Ukraine) dans leurs efforts pour développer leurs capacités en matière de cybersécurité aux niveaux national et régional. La GFA travaille en partenariat avec l'Académie estonienne de l'e-gouvernance, Detecon International, Action Global et l'Office fédéral allemand de la sécurité de l'information (BSI).

En même temps, le projet vise à faciliter l'harmonisation juridique et institutionnelle et le rapprochement des pays du partenariat oriental avec l'Union européenne en se concentrant sur le rapprochement avec la directive de l'UE sur les réseaux et les systèmes d'information (NIS). Les deux composantes comprennent le renforcement de la gouvernance et des cadres juridiques nationaux en matière de cybersécurité, et l'élaboration de cadres pour la protection des opérateurs de services essentiels (OES) et des infrastructures d'information critiques. Un autre volet consiste à accroître les capacités opérationnelles de gestion des incidents de cybersécurité des équipes nationales, respectivement gouvernementales, d'intervention en cas d'urgence informatique (CERT).

Un autre volet du projet portant sur la prévention et la poursuite de la cybercriminalité est mis en œuvre en parallèle par le Conseil de l'Europe (CoE). Cela permet à GFA de rechercher des synergies et d'examiner les liens étroits entre la cybersécurité et la cybercriminalité. Pour atteindre ses objectifs, le projet répond aux besoins spécifiques de chacun des pays du partenariat oriental tout en favorisant le développement des capacités et la coopération au niveau régional entre les six pays du partenariat oriental, et entre ces derniers et les États membres de l'UE et les institutions européennes.

L'APPROCHE ET LA STRATÉGIE DE GFA

Les six pays du partenariat oriental continuent de progresser sur différents aspects de la cybersécurité mis en évidence, par exemple, dans l'indice mondial de cybersécurité de l'Union internationale des télécommunications pour 2018/19. Cependant, les pays présentent des différences et des défis considérables en ce qui concerne leur niveau de cyber-résistance. Un projet ayant une portée régionale et une orientation technique aussi larges doit tenir compte de ces différences avec soin afin de fournir des mesures de développement des capacités significatives et complètes. Un autre facteur est la diversité des niveaux de coopération entre les différents pays du partenariat oriental et entre ces derniers et l'UE. Par exemple, la Géorgie, la Moldavie et l'Ukraine ont signé des accords d'association ainsi que des accords de libre-échange approfondis et complets avec l'UE, alors qu'aucun accord de ce type n'est en place avec le Belarus, l'Azerbaïdjan et l'Arménie. Ces différences ont des implications directes sur les besoins spécifiques des pays en matière de soutien technique ainsi que sur les possibilités de renforcer le rapprochement de leurs cadres juridiques nationaux avec ceux de l'UE pour la cybersécurité et la directive NIS. La stratégie du projet GFA se concentre donc sur des activités différenciées et sur mesure, basées sur une analyse solide et approfondie du statu quo au niveau national et régional.

ACTIVITÉS ACTUELLES DU PROJET

La collecte d'informations de base détaillées pour chacun des six pays est une étape clé du projet afin de comprendre et d'évaluer correctement leur situation respective en matière de cybersécurité. À cet effet et afin de présenter le projet aux partenaires et bénéficiaires de la coopération locale, l'équipe d'experts du GFA a commencé à effectuer des missions dans tous les pays du partenariat oriental.

En janvier, le chef de l'équipe GFA a participé à la première réunion du comité directeur du projet CyberEast, géré par le Conseil de l'Europe, à Kiev, en Ukraine, qui a permis de coordonner les approches des deux projets, de rencontrer toutes les organisations partenaires concernées et de commencer par la collecte de données et d'informations de base.

La première mission en Ukraine a été suivie par des missions initiales en Moldavie, au Belarus et en Arménie en février et mars. En Moldavie, le projet prévoit de soutenir la poursuite de la qualification et du renforcement organisationnel des CERT du gouvernement, la révision des cadres de protection des infrastructures critiques ainsi que la sensibilisation des citoyens à la cyberhygiène. La situation actuelle en Arménie offre au projet la possibilité de faciliter les efforts nationaux

LA DIRECTIVE NIS EUROPÉENNE

La directive européenne sur la sécurité des réseaux et des systèmes d'information (NIS), adoptée en 2016, est la pièce maîtresse de la stratégie de l'UE en matière de cybersécurité et présente la première législation européenne complète sur la cybersécurité. Elle vise à atteindre un niveau minimum d'harmonisation entre les États membres en les obligeant à adopter des stratégies nationales en matière de NEI et à créer des points de contact uniques ainsi que des CERT. En outre, il définit les exigences de sécurité et de notification pour les OES dans des secteurs critiques tels que l'énergie, la banque, les infrastructures numériques, les transports, l'eau, la santé, etc. et permet une collaboration transfrontalière grâce à un réseau de CERT et au groupe de coopération stratégique NIS. La réduction de la cybercriminalité est un autre objectif clé de la directive NIS.

CYBERSÉCURITÉ ET CYBERCRIMINALITÉ

CYBERSÉCURITÉ STRATÉGIES

SÉCURITÉ ▪ CONFIANCE ▪ RÉSILIENCE ▪ LA FIABILITÉ DES TIC

INCIDENTS DE SÉCURITÉ NON INTENTIONNELS LIÉS AUX TIC

catastrophes
défaillance technique
erreur humaine

*TCI: Technologies de l'information et de la communication

LES ATTAQUES INTENTIONNELLES CONTRE LES TIC PAR :

ÉTAT ACTEURS | AC-TEURS NON ÉTA-TIQUES | TERRO-RISTES | CRIMINELS

INFRASTRUCTURE CRITIQUE ATTAQUES

AUTRE ATTAQUES SUR LA CONFIDENTIALITÉ, L'INTÉGRITÉ ET LA DISPONIBILITÉ DES TIC

CYBERCRIMINALITÉ STRATÉGIES

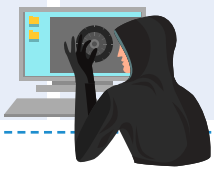
ÉTAT DE DROIT ▪ JUSTICE PÉNALE ▪ DROITS DE L'HOMME

INFRACTIONS PAR LE BIAIS DES TIC

INFRACTIONS IMPLIQUANT LES TIC

L'UTILISATION FRAUDULEUSE ET TERRORISTE DES TIC
Infractions aux DPI
l'extorsion...

TOUT INFRACTION IMPLIQUANT DES PREUVES



Premier comité directeur du CyberEast 13-14 février 2020 à Kiev, Ukraine

visant à élaborer une stratégie nationale de cybersécurité et de soutenir la mise en place d'un nouveau CERT national. Au Belarus, aider à l'élaboration d'un document de stratégie nationale en matière de cybersécurité peut ne pas être possible en raison du calendrier relativement étroit et de la nature du sujet, qui est politiquement chargé. Toutefois, en collaboration avec les parties prenantes à Minsk et le CERT national, un certain nombre de priorités conformes aux objectifs du projet ont été identifiées. Ces derniers comprennent, par exemple, une campagne de cyberhygiène et un soutien à la capacité technique des CERT existants et sectoriels qui doivent encore être créés.

En Géorgie, le projet a pu s'adapter rapidement à la crise de coronavirus et entamer une collaboration avec son projet frère mis en œuvre par le CdE. Ce projet soutient les efforts de réforme en cours du gouvernement pour revoir et améliorer le cadre juridique de la cybercriminalité et de la cybersécurité. En même temps, l'étude de base du contexte national plus large est préparée sous forme de recherche documentaire, qui sera complétée par une première mission dans le pays à un stade ultérieur.

Toutes les missions effectuées et les parties prenantes engagées ainsi que les informations et les données recueillies montrent le grand intérêt des homologues de GFA ainsi que le fait que le projet démarre au bon moment. La cybersécurité est un sujet de grande importance pour la Commission européenne (CE) qui a lancé plusieurs initiatives dans ce domaine ces dernières années, dont le CyberNet de l'UE. Ce dernier a été lancé par la Direction générale de la coopération internationale et du développement de la Commission en septembre 2019. Il vise à renforcer la mise en œuvre, la coordination et la cohérence au niveau mondial des projets de développement de la cybercapacité de l'UE au cours des quatre prochaines années et à renforcer la capacité de l'UE à fournir une assistance technique aux pays tiers en matière de cybersécurité et de cybercriminalité. Le réseau de renforcement des capacités en matière de cybersécurité est mis en œuvre sous les auspices de l'autorité estonienne chargée des systèmes d'information, en partenariat avec l'autorité luxembourgeoise chargée de la cybersécurité, l'agence finlandaise des transports et des communications et le ministère fédéral allemand des affaires étrangères.

En raison des restrictions induites par coronavirus, plusieurs projets EU4Digital en cours ont lancé une série d'ateliers virtuels hébergés par la CE, qui offre une plateforme à tous les chefs d'équipe EU4Digital pour présenter leurs projets respectifs, échanger des expériences et présenter des solutions pour relever les défis communs liés au Covid-19. En outre, les principaux intermédiaires des projets des pays du partenariat oriental ont participé aux ateliers. Cela a permis au projet de souligner l'importance de l'OES comme l'une de ses caractéristiques centrales et de discuter des meilleures pratiques concernant les questions de sécurité, y compris les infrastructures et les services du secteur de la santé. Les tentatives des criminels de promouvoir et de vendre en ligne des médicaments et du matériel médical contrefaits prouvent encore la nécessité et l'urgence de sensibiliser les citoyens à la cyberhygiène, autre objectif important du projet.

En mars 2020, la CE a invité GFA à participer à un atelier de deux jours à Bruxelles, à présenter son approche et à échanger avec ses collègues et les parties prenantes européennes sur l'état des lieux des approches de renforcement des capacités liées à la cybersécurité. L'équipe de GFA a ainsi eu l'occasion de se mettre en réseau et d'apprendre avec et de la part d'autres personnes impliquées dans ce domaine en évolution rapide.

Contact : Tobias Tschappe,
tobias.tschappe@gfa-group.de &
Rune Rossius, rune.rossius@gfa-group.de

UNE VOIX DU PROJET SUR LES IMPLICATIONS DE COVID-19 PAR BESNIK LIMAJ, CHEF DE L'ÉQUIPE GFA

Malgré les circonstances, notre projet s'efforce toujours de produire les résultats de sa période de lancement. Bien que les événements et les réunions en face à face ne puissent pas avoir lieu actuellement, le travail et les réunions en ligne se poursuivent. L'équipe du projet GFA travaille 24 heures sur 24 pour aider nos partenaires et la CE à faire face à la crise de coronavirus.

Les six pays partenaires sont confrontés à de graves difficultés car les cyberattaques et les activités frauduleuses ont augmenté depuis l'épidémie de coronavirus. Nous sensibilisons donc nos bénéficiaires et nos partenaires à la nécessité d'être particulièrement vigilants face aux escroqueries en ligne, y compris le phishing et les logiciels malveillants. Nous avons élaboré des recommandations à l'intention des CERT des pays partenaires et des employés de leurs mandants sur la manière d'assurer la sécurité en ligne lors de l'utilisation d'appareils et de systèmes numériques. Cela inclut des conseils sur diverses questions : L'utilisation d'un réseau privé virtuel (VPN), des politiques de déconnexion automatique lorsqu'on s'éloigne des ordinateurs, un accès limité aux appareils lorsqu'on les utilise uniquement pour le travail, des rappels sur la mise à jour des logiciels, y compris le pare -feu et les programmes antivirus, la sauvegarde des données, la possibilité d'une authentification à deux ou plusieurs facteurs et l'utilisation de mots de passe forts et longs pour l'accès en ligne.

En outre, nos recommandations accordent une attention particulière à l'hameçonnage des courriels, car environ 90 % de toutes les cyberattaques commencent par des courriels. Les bénéficiaires des pays partenaires doivent donc considérer la protection du courrier électronique comme une première ligne de défense et être en mesure de faire tout ce qu'il faut pour empêcher les courriers électroniques malveillants d'atteindre leurs appareils.

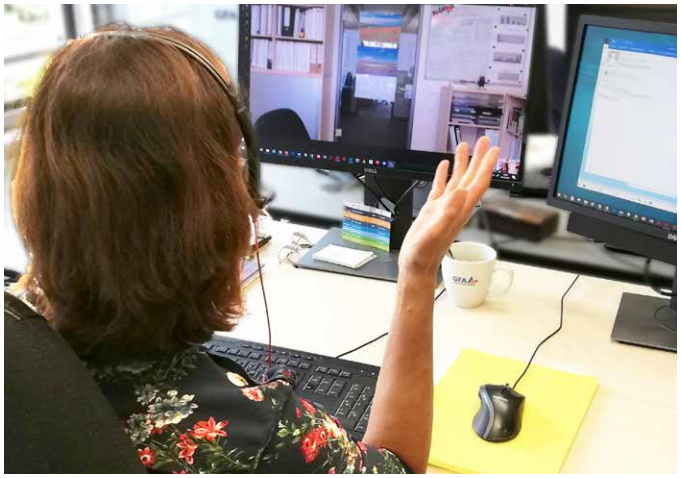
Dans l'ensemble, nous avons pu tirer les leçons des événements extrêmes de ces dernières semaines et nous pouvons faire face aux menaces de cybersécurité lorsque des acteurs criminels tentent de tirer profit de la pandémie de Covid-19.

UN ÉCHANTILLON DES RÉPONSES NUMÉRIQUES DE GFA À LA PANDÉMIE DE CORONAVIRUS

Mandaté par le projet sectoriel de la GIZ Enseignement et formation techniques et professionnels (EFTP), le département Éducation, compétences et emploi de GFA réalise une étude sur l'application des formats d'apprentissage numériques dans le secteur de l'EFTP en réponse au Covid-19. L'étude se penche sur les pays partenaires de la coopération allemande au développement et présente des approches numériques créatives qui compensent les cours annulés. Elle identifie les besoins et les lacunes des applications numériques. Sur la base de ces cas, GFA développera des approches dans les systèmes d'EFTP des pays partenaires qui intègrent systématiquement des formats d'apprentissage numériques.

En raison de la pandémie de coronavirus, GFA connaît une poussée de numérisation au sein de sa propre organisation. Comme les équipes des États membres ont été testées plus tôt cette année, cela a permis à GFA de déployer l'application dans toute l'entreprise en quelques jours. À ce jour, les coordinateurs de projet sont non seulement capables de communiquer et de travailler ensemble depuis leur domicile, mais les défis techniques, les réponses au coronavirus et les meilleures pratiques sont affichés, discutés et mis en pratique collectivement dans tous les services et la hiérarchie des postes. GFA est impatiente d'exploiter davantage les possibilités de communication interne et de gestion des connaissances au cours des prochains mois.

GFA a lancé ses procédures d'intégration des nouveaux employés en passant au numérique. L'entreprise organise désormais son premier jour de travail d'introduction aux ressources humaines et la majorité des cours d'accueil en ligne via MS Teams. Les cours d'embarquement sont précédés d'une courte introduction à la formation en ligne sur MS Teams. Tous les nouveaux employés se présentent sur le site Web interne de GFA et sont invités à participer aux chaînes correspondantes de MS Teams. Par ailleurs, GFA a récemment lancé une série de webinaires intitulée « GFA Learns Digital » à l'intention des coordinateurs et du personnel des projets du monde entier. Plus de 60 participants ont suivi une brève et intense intervention d'une heure sur le moment et la manière d'utiliser les outils en ligne pour le vote et les présentations en direct. D'autres webinaires et la production de guides rapides pour le travail à distance ont suivi, conformément aux besoins de 164 projets GFA en cours, recueillis par le biais d'une enquête. En outre, un soutien individuel aux équipes de projet a été mis en place ainsi qu'une assistance par groupes de pairs pour un transfert rapide de connaissances entre les projets.



La GFA, en coopération avec la European Digital SME Alliance, a récemment proposé un webinaire intitulé « Digital Solutions in Times of Covid-19 » dans le cadre du projet Dialogue sur la diversification économique entre l'UE et le Conseil de coopération du Golfe (CCG), financé par l'Instrument européen de politique étrangère. Le webinaire était gratuit et a permis de présenter aux parties prenantes du projet la première et la plus grande association de PME d'Europe spécialisée dans les TIC et le soutien qu'elle offre aux PME et aux startups. Par exemple, l'association a lancé une campagne pour partager les solutions numériques offertes par les PME et les startups avec des clients publics et privés qui ont besoin de nouveaux outils et services pour atténuer les effets de la crise du Covid-19. Le projet de dialogue UE-CCG en général contribue à renforcer les relations entre l'UE et le CCG en soutenant le processus de diversification économique en cours dans les pays du CCG, qui s'éloigne des secteurs dépendant des hydrocarbures. Ces dernières semaines, le projet est devenu plus pertinent que jamais car les modèles de diversification économique dans le CCG sont basés sur des services orientés vers les clients tels que le tourisme, les transports, la promotion immobilière et les services financiers qui sont fortement touchés par la crise. De plus amples informations sur le projet ainsi que sur les développements récents dans l'UE et le CCG sont disponibles à l'adresse suivante :

www.linkedin.com/company/eu-gcc-dialogue-on-economic-diversification

www.digitalsme.eu/solutions

Contact : Anja Desai, anja.desai@gfa-group.de

MENTIONS LÉGALES

Newsletter de GFA établie par GFA Consulting Group GmbH, Eulenkrugstraße 82, D-22359 Hambourg, Allemagne, tél. : +49 (0) 40 603 06-100, fax : +49 (0) 40 603 06-199, e-mail : newsletter@gfa-group.de, www.gfa-group.de, tous droits réservés © 2020, responsable du contenu : Anja Desai, édité par Manfred Oepen, ACT Assist GmbH, mise en page : Natascha Pleß, photos : GFA, istockphoto

gfagroup GFA_CG gfa-consulting-group-gmbh gfaconsultinggroup

GFA Consulting Group est une société de conseil en pleine croissance qui aide au développement économique international. Les principaux secteurs de l'entreprise comprennent l'agriculture & le développement rural, la gestion des ressources naturelles & l'environnement, le changement climatique, l'énergie, la gouvernance, la gestion des finances publiques, le développement du secteur privé, l'éducation, les compétences & l'emploi, le développement de systèmes financiers, la santé, l'innovation numérique, la surveillance et l'évaluation, l'eau, l'assainissement & gestioin des déchets et contrats cadres. Chaque année, GFA réalise environ 300 projets et études à travers le monde.

La vision de GFA – être le partenaire de choix de nos clients dans nos principaux domaines de service.

La mission de GFA – améliorer les moyens d'existence des bénéficiaires grâce à nos services professionnels.

Les valeurs-clés de GFA – proposer des prestations de services performantes, l'excellence technique dans nos principaux secteurs d'activité, des produits et approches innovants et une crédibilité auprès de nos clients dans la mise en œuvre de leurs projets.