Sur votre blog, Professeur Ziccardi, vous avez parlé de l'importance d'être le premier à protéger ses données, en commençant par exemple par l'authentification à deux facteurs.

Quels conseils donneriez-vous à un internaute et consommateur pour être le plus protégé possible dans l'environnement numérique ?

Ziccardi : Oui, le moment de l'authentification, c'est-à-dire l'accès à toutes nos données et systèmes, est encore très sous-estimé. Nous portons avec nous l'idée d'un mot de passe depuis près de cent ans et il faut l'oublier, préférant les systèmes qui demandent plus de vérifications, de la part de l'individu, pour lui permettre d'accéder à ses données.

Augmenter les facteurs nécessaires (en utilisant, par exemple, des OTP, des cartes, des téléphones portables ou des applications spécifiques) augmente par conséquent notre sécurité. Le monde bancaire a été le premier, au cours des dernières années, à forcer cette migration vers des systèmes d'authentification plus forts et les résultats ont été constatés en termes de sécurité.

- Je recommanderais donc une authentification forte et une redondance constante de nos données, avec des sauvegardes effectuées en temps réel et à plusieurs endroits.
- Cela nous protège à la fois d'éventuelles attaques et d'accidents.Toujours sur votre blog, professeur Ziccardi, vous écrivez qu'une grande partie de la protection des données implique également une série de comportements humains "corrects".

Pourriez-vous mieux expliquer ce que vous entendez par là ?

Ziccardi : C'est une question de sécurité humaine. Très souvent, il est plus facile d'attaquer le cerveau des gens, d'entrer dans leur ordinateur ou leur téléphone, que l'appareil informatique lui-même. Si les gens sont obligés de se comporter de manière incorrecte, les portes du système s'ouvrent.

Pensez à une personne qui clique sur un lien frauduleux, qui ouvre une pièce jointe contenant un virus, qui récupère une clé USB contenant un cheval de Troie et l'insère dans son ordinateur portable, ou à un utilisateur qui se contente de fournir, par e-mail, des informations utiles pour accéder à son systèmes.

Dans le cadre de la pandémie, les cyberattaques ciblant les comportements ont donc considérablement augmenté à mesure que les gens sont devenus encore plus tendus et vulnérables.

- **Quelle est la situation aujourd'hui en matière de cybersécurité ?** Même face à l'actualité ces derniers jours selon laquelle Linkedin, une plateforme utilisée par des millions d'utilisateurs à travers le monde, a été victime d'une violation de données, avec les données d'environ 700 millions d'utilisateurs en danger (92% des utilisateurs).
- Scorza : Les meilleurs de mes amis qui s'occupent de la cybersécurité ne cessent de me rappeler que la sécurité, vraie et absolue, n'existe pas.
- Il n'y a toujours pas d'unanimité sur le fait que Linkedin a effectivement subi une violation mais, somme toute, peu importe car même des violations de données importantes sont à l'ordre du jour.

- Je n'aime pas me répéter mais, même dans ce cas, je ne pense pas qu'il s'agisse d'un match technologique ou, du moins, d'un match qui peut être gagné simplement grâce à la technologie.

Nous devons éduquer les personnes, les entreprises et les administrations sur la valeur des données - personnelles et autres - car dans la plupart des cas, nos esprits sont plus vulnérables que nos systèmes informatiques.

Ziccardi : C'est une situation complexe. La pandémie a ensuite conduit, dans de nombreux domaines, à une crise économique, et les premières coupes ont eu lieu dans ce domaine, notamment pour les petites et moyennes entreprises.

La sécurité coûte en effet très cher. Il existe également un problème de cybersécurité dans de nombreuses structures publiques, qui paient le fait qu'elles n'ont pas prévu, ces dernières années, des plans d'action ordonnés et méthodiques en ce sens.

Outre les investissements, une formation spécifique et ciblée de tous ceux qui traitent les données devient essentielle.

Dans ce cas également, de nombreux plans de formation n'ont jamais abouti, générant une vulnérabilité « congénitale » dans de nombreuses structures.Le rapport d'activité 2020 du garant de la vie privée vient d'être publié, avec un grand focus sur la protection des mineurs sur les plateformes sociales telles que Tik Tok, le revenge porn et le cyberharcèlement.

Avvocato Scorza, comment le Garant aide-t-il les consommateurs à se protéger contre ces éventuelles menaces en ligne ?Zeste : Nous faisons de notre mieux même si, j'avoue, que parfois la sensation est celle de saint Augustin devant le célèbre enfant qui voulait vider la mer avec un seau.

Nous essayons d'éduquer les jeunes pour qu'ils ne soient pas victimes de ce genre de phénomènes et, dans tous les cas, lorsque quelque chose ne va pas - car malheureusement, il est inévitable que cela puisse arriver - de contacter le.

Garant pour obtenir de l'aide

Ces infractions sont trop le même, qui génèrent également une souffrance énorme chez les plus petits ne sont même pas signalés.Et puis on travaille un peu sur la technologie : grâce à un accord récent avec Facebook et Instagram par exemple, on est aujourd'hui capable de bloquer préventivement la mise en ligne d'une vidéo à fond sexuel et donc où le consentement de la personne dépeint là, d'une vidéo porno de vengeance.