23.06.2022 – 10:30 Uhr

Communiqué de presse Swissmem : Attaques illégales : 70% des entreprises membres de Swissmem sont concernées

Zurich (ots) -

Attaques illégales : 70% des entreprises membres de Swissmem sont concernées

À l'époque de la numérisation les entreprises industrielles sont fortement menacées par la cybercriminalité. Tant les cyberattaques que les attaques physiques représentent aujourd'hui une menace continue. Cela peut toucher chaque entreprise, quelle que soit sa taille. Le potentiel de dommages est énorme et peut, dans les cas extrêmes, mettre en péril l'existence même d'une entreprise. Une enquête menée par Swissmem auprès des entreprises membres montre qu'au cours des deux dernières années, 70% des entreprises ayant répondu au sondage ont été victimes d'au moins une attaque. Par conséquent, les entreprises sont très sensibilisées à ces risques. Pratiquement toutes les entreprises mettent en oeuvre des mesures de prévention ciblées. Grâce à ces mesures, 82% des attaques considérées comme très graves n'ont pas eu de conséquences ou ont pu être résolues à court terme. Il s'agit cependant de ne pas relâcher l'attention.

En collaboration avec l'Institut de droit pénal et de criminologie de l'Université de Berne, Swissmem a mené une enquête auprès de ses 1 200 entreprises membres sur les questions de sécurité. 271 entreprises ont rempli le questionnaire. Les réponses montrent qu'au cours des deux dernières années, 70% des entreprises ayant répondu au sondage ont été victimes d'au moins une attaque. Certaines entreprises ont été attaquées plus de 20 fois.

Avec 50%, la fraude liée au CEO a été le genre d'attaque le plus fréquent. Dans ce contexte, les criminels tentent d'obtenir des transferts d'argent en utilisant une fausse identité. 43% ont indiqué avoir été victimes d'attaques par hameçonnage. L'objectif de ces attaques consiste à accéder aux systèmes TIC afin d'obtenir illégalement des données précieuses. Un membre de Swissmem sur cinq (20,7%) a été victime de logiciels malveillants tels que des virus, des vers et des chevaux de Troie, ainsi que d'attaques sous forme de piraterie informatique. Une entreprise sur six a été concernée par une attaque d'ingénierie sociale (16,2%). Dans ce cas, le but est d'espionner les collaborateurs de manière ciblée afin d'obtenir des informations confidentielles. La majorité des entreprises attaquées (58,3%) supposent toutefois qu'elles ont été touchées par hasard. Plus d'un cinquième des entreprises concernées (21,4%) supposent par contre qu'elles ont été attaquées de manière ciblée.

Les deux responsables d'études de l'Université de Berne, le professeur Ueli Hostettler et Anna Isenhardt, ont remarqué que : " les entreprises qui ont répondu sont particulièrement touchées par des attaques du domaine de la cybercriminalité. Comparé à d'autres délits, ce type de délit a augmenté à l'échelle internationale ces dernières années. Un très grand nombre d'attaques liées à la cybercriminalité, signalées depuis l'existence de l'entreprise, ne semblent avoir eu lieu qu'au cours des deux dernières années. "

Les entreprises membres de Swissmem savent que les attaques illégales peuvent avoir de graves conséquences. Cela vaut aussi bien pour les grandes entreprises que pour les PME. En moyenne, elles utilisent 25 mesures de protection et d'intervention. Grâce à ces mesures, 82% des incidents n'ont pas eu de conséquences (13,7%) ou ont pu être résolues à court terme (68,4%). Toutefois pour une entreprise sur six (15,8%), l'attaque a entraîné des restrictions opérationnelles considérables. Ce sont notamment les attaques du domaine de la cybercriminalité qui peuvent avoir des conséquences graves et coûteuses. Pour pratiquement un cinquième des entreprises interrogées (18,2%), les attaques ont causé des dommages entre 100 000 et un million de francs. Selon l'entreprise, cela risque de menacer son existence.

Martin Hirzel, président de Swissmem, commente les résultats de l'enquête : " Je constate avec plaisir qu'au sein des membres de Swissmem, il existe une forte sensibilisation aux cyberattaques et aux menaces physiques. Il s'agit cependant de ne pas relâcher l'attention. Chaque entreprise doit toujours être préparée au niveau technologique et organisationnel afin de pouvoir contrer de telles attaques. Ce domaine est l'affaire du chef ".

Numérisation ou cybersécurité

Face à ce scénario, de nombreuses entreprises industrielles se voient confrontées à un conflit d'objectifs. D'une part, elles sont appelées à investir dans la numérisation des processus, produits et services de l'entreprise. Pour cela, elles ont besoin de faire partie d'un réseau de plus en plus performant au niveau des systèmes qui dépasse parfois les limites de l'entreprise. D'autre part, la protection de ces systèmes doit avoir lieu avec précaution, notamment lors de la mise en réseau, et demande la mise en oeuvre de mesures de blindage appropriées.

L'initiative " Industrie 2025 " peut aider à résoudre ce conflit d'objectifs. Elle est parrainée par les associations Swissmem, asut et SwissTnet. Son objectif est de faire progresser la transformation numérique sur la place industrielle suisse. Une offre spéciale appelée " Security 2025 " est proposée aux entreprises industrielles. Des experts aident en particulier les PME à aborder les thèmes de la sécurité de manière appliquée et pratique. Ils prennent particulièrement en considération les besoins de l'industrie mis en réseau.

Contact:

Pour tout renseignement :

Jonas Lang, suppléant du chef de division
Tél. +41 44 384 48 33 / portable +41 79 777 41 36
E-Mail: j.lang@swissmem.ch

Philippe Cordonier, Responsable Suisse romande
Tél. +41 21 613 35 85 / portable +41 79 644 46 77
E-mail : p.cordonier@swissmem.ch