Lutter contre les menaces dans un monde de plus en plus numérisé

Par Wolfgang Picot

En mai 2022, l'Institut autrichien de technologie (AIT) est devenu le premier centre collaborateur de l'Agence internationale de l'énergie atomique (AIEA) en matière de sécurité de l'information et de sécurité informatique pour la sécurité nucléaire. L'AIT appuie les cours et les exercices régionaux et internationaux sur la sécurité informatique pour les installations et activités nucléaires, élabore des modules de démonstration technique pour sensibiliser aux cybermenaces et contribue à l'élaboration de matériel de formation pour le Centre de formation et de démonstration en matière de sécurité nucléaire à Seibersdorf.

Pour mieux comprendre cette coopération, nous nous sommes entretenus avec Helmut Leopold, directeur du Centre pour la sûreté et la sécurité numériques de l'AIT.

Quels sont les risques et les menaces qui se font jour dans le domaine de la sécurité informatique en général ?

Aujourd'hui, de nombreux appareils numériques modernes sont construits en vue de réseaux plus étendus. Nombre d'entre eux ont besoin d'un accès à internet pour fonctionner. Le développement de chaque logiciel comporte toujours un risque d'erreurs pouvant conduire à des vulnérabilités. Des interfaces mal protégées et des utilisateurs irresponsables augmentent le nombre de menaces de sécurité pour l'exploitation des systèmes de technologie de l'information (TI).

Les attaquants exploitent les vulnérabilités des systèmes numériques pour y accéder. Les méthodes et outils des attaques évoluent avec les processus d'innovation numérique. Des logiciels pour pirates informatiques sont maintenant facilement disponibles sur internet, ce qui rend les attaques plus faciles même pour les moins doués d'entre eux. Nous sommes confrontés à un écosystème de cyberattaques diversifié mû par le crime organisé, l'espionnage économique et industriel et le cyberterrorisme.

Ainsi, aujourd'hui, un large spectre de cyberattaques menace les utilisateurs, les entreprises et les autorités, et peut toucher l'infrastructure numérique d'États entiers en même temps que des campagnes de désinformation ciblées, ébranlant les bases de nos sociétés.

Le secteur nucléaire est-il confronté aux mêmes dangers ?

Les entreprises et les particuliers utilisent des technologies de l'information (TI) qui sont avant tout basées sur les données et la communication. En revanche, les installations de production et les infrastructures essentielles utilisent des technologies dites d'exploitation qui surveillent et contrôlent les comportements et les résultats de processus de production définis. Les technologies d'exploitation sont traditionnellement beaucoup moins interconnectées que les TI. Cependant, avec les progrès technologiques, les deux domaines ont convergé, et les logiciels et dispositifs des technologies d'exploitation sont de plus en plus connectés à des réseaux plus vastes.

Cette évolution pose problème, car la sensibilisation à la cybersécurité est moins répandue dans le domaine des technologies d'exploitation que dans celui des TI.

Par conséquent, ces nouvelles menaces pour la sécurité des TI deviennent pertinentes pour les technologies d'exploitation utilisées pour la production industrielle et les infrastructures essentielles. Il en va de même pour le secteur nucléaire, qui avait traditionnellement une approche conservatrice et maintenait des systèmes de contrôle isolés.

Commet agit l'AIT pour renforcer la cybersécurité dans le domaine de la sécurité nucléaire ?

Le programme de recherche de l'AIT étudie l'incidence des scénarios de menace en évolution sur les systèmes des technologies d'exploitation et vise à mettre au point un savoir-faire et de nouvelles solutions pour accroître la résilience des infrastructures essentielles face aux cyberattaques. Ces travaux servent à élaborer de nouvelles normes de sécurité mondiales, des procédures de certification pour les éléments essentiels des systèmes et des nouvelles architectures de systèmes afin d'intégrer de solides mesures de cybersécurité dans les systèmes des technologies d'exploitation dès le début de leur conception.

L'AIT propose également une formation complète pour préparer aux attaques de cybersécurité. Dans des simulations complexes de systèmes de TI « virtualisés », les utilisateurs, les développeurs de systèmes, le personnel d'exploitation et les représentants des gouvernements réagissent à des scénarios réalistes de cyberattaque. Ces simulations sont essentielles pour garantir la résilience des systèmes de TI et des technologies d'exploitation et leur capacité à lutter efficacement contre les cybermenaces.

Quels sont les avantages de l'environnement d'apprentissage virtuel mis au point par l'AIT et l'AIEA ?

L'expérience pratique est le mode d'apprentissage le plus efficace. L'AIT et l'AIEA ont mis au point une simulation qui permet de créer des « jumeaux numériques » d'infrastructures numériques essentielles existantes et qui forme également à des scénarios d'application très réalistes.

Dans cet environnement virtuel, les utilisateurs des secteurs public et privé peuvent évaluer et tester l'efficacité des mécanismes de protection et des processus opérationnels.

L'expérience tirée de cet environnement d'apprentissage virtuel contribue à la mise en place de capacités défensives durables dans les organisations publiques et privées.

Outre la formation virtuelle, comment les travaux et l'expertise de l'AIT en sécurité informatique font-ils progresser la sécurité nucléaire ?

Nous pouvons contribuer à la défense contre les attaquants, par exemple en mettant au point des logiciels pour surveiller les périphériques de périmètre qui relient généralement les réseaux internes des organisations à internet. Les attaquants se servent souvent de ces systèmes comme porte d'entrée avant de faire des dégâts.

Nous mettons à profit notre expérience de la détection des anomalies pour entraîner des logiciels d'analyse qui surveillent ces périphériques de périmètre généralement utilisés dans un type particulier d'installation nucléaire.

Un tel logiciel peut déclencher une alarme ou prendre des contre-mesures si un périphérique se comporte de manière anormale. Ainsi, les exploitants peuvent rapidement détecter et bloquer les cyberattaques avant qu'elles ne causent des dommages importants.

Il y a un an l'AIT a été désigné premier centre collaborateur de l'AIEA dans le domaine de la sécurité informatique pour la sécurité nucléaire et reste aujourd'hui le seul centre de ce type. Qu'est-ce que cela implique pour le travail de l'AIT ?

Nous sommes extrêmement fiers d'avoir été désignés centre collaborateur et nous continuons à appuyer l'organisation d'un cours régional sur la sécurité informatique pour les systèmes d'instrumentation et de contrôle dans le secteur nucléaire. Le cours a été organisé deux fois en 2022 et a utilisé certains résultats de notre entreprise commune pour élaborer une plateforme de formation virtuel.

Nous avons également participé à des activités sur la sécurité informatique dans le cadre de la mise au point de petits réacteurs modulaires.

En ce moment, nous aidons l'AIEA à préparer la conférence internationale de 2023 sur la sécurité informatique dans le monde nucléaire : la sécurité pour la sûreté, où nous ferons des démonstrations de notre plateforme de formation virtuelle, présiderons des tables rondes et présenterons des documents sur nos recherches dans le secteur, et plus encore.

Comment l'AIT participe-t-il au Centre de formation et de démonstration en matière de sécurité nucléaire ?

Nous avons travaillé en étroite collaboration avec nos collègues de l'AIEA pour mettre au point des modules de formation, des démonstrations et des exercices pour ce centre. Nous intégrons des modules de sécurité informatique aux cours sur la protection physique des matières nucléaires et des autres matières radioactives, et sur la détection et l'intervention au cas où des matières nucléaires et d'autres matières radioactives échappent au contrôle réglementaire. Ce fonctionnement vise à renforcer l'idée que la sécurité informatique est une partie intégrante et indissociable de la sécurité nucléaire.