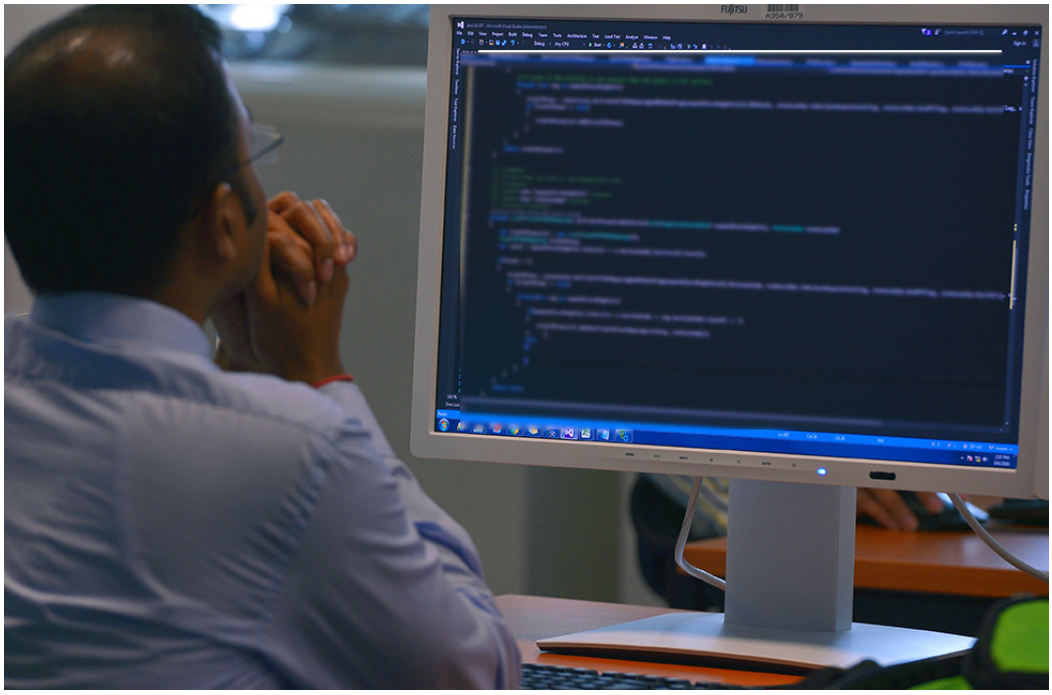
Guns, guards, gates and geeks: Romania strengthens computer security at nuclear installations

By Laura Gil



(Photo: D. Calma/IAEA)

A cyberattack could swipe all the information stored on your computer or even prevent it from working. That's bad enough. But a cyberattack on a nuclear power plant could lead to sabotage or theft of nuclear material. Computer security, concerned with the protection of digital data and the defence of systems and networks against malicious acts, is a critical component of nuclear security.

"The advance of computers and their use in all aspects of nuclear operations has changed the security paradigm," said Donald Dudenhoeffer, Information Technology Security Officer at the IAEA. "Information and computer security must be considered as components in the overall nuclear security plan."

Nuclear security has long been dominated by a focus on physical protection — often referred to as guns, guards and gates — but today's criminals have also embraced computers as a means and target of attacks. A cyberattack could lead to the loss of nuclear security information, the sabotage of nuclear installations and, combined with a physical attack, the theft of nuclear or other radioactive material. Computers now play an essential role in the safety, security and management of nuclear facilities; it is of vital importance that all systems are properly secured against malicious intrusions.

"We all need to be prepared to defend ourselves from the non-benign environment of the internet and the digital age," Dudenhoeffer said. "We all use computers, and we all need to build greater awareness of the threats, risks and means for protection." Regulators and operators of nuclear installations are increasingly aware of the importance of computer security and are seeking to enhance their nuclear security programmes. Romania, according to Dudenhoeffer, is one exemplary case.

"We understand the importance of protection against all kinds of threats that may affect the safe, secure and reliable operation of our nuclear installations, including threats directed at computer and information security," said Madalina Tronea, Coordinator at the Nuclear Regulations and Standards Unit of the National Commission for Nuclear Activities Control (CNCAN) in Bucharest, Romania.

In 2012, a group of IAEA specialists conducted an International Physical Protection Advisory Service mission in Romania. They provided the authorities with a list of recommendations to further develop an adequate regulatory framework for the protection of nuclear installations against various threats, including cyberattacks.

Shortly afterwards, a team of nuclear regulators from the CNCAN started working on a regulation that came into force in November 2014. The regulation focuses on the protection of systems, equipment and components — including software for instrumentation and control systems — that are important to nuclear safety, security, safeguards and emergency response. In addition to the regulation, the CNCAN issued a document outlining cyberthreats taking into account new threats and recent computer security events in industry around the world.

"We pay attention to the global context and to the changes in both threats and countermeasures," Tronea said. "And we do our best to ensure an adequate prevention and protection against computer security incidents as well as effective response to such events, should they occur."

In that same year, the Romanian Government approved a National Strategy for Nuclear Safety and Security, which includes objectives dedicated to the continuous improvement of computer security in the nuclear sector.

People: the problem and the solution

Studies show that the majority of computer security incidents are caused by human errors.

"People: human capacity development is one of the best investment areas," Dudenhoeffer said. "We don't need a world filled with experts in computer security. We need a world filled with people who are aware of the computer security risks and basic measures of defence. We need a well-informed workforce and leadership."

Thanks to the IAEA training courses that Romania has participated in since 2013, the country has built a sustainable network of stakeholders. Through the network, stakeholders now share experiences in nuclear security and work together to build

(Photo: CNCAN)

robust information and computer security programmes.

Through national training courses, online learning, expert meetings and train-the-trainer programmes, the IAEA works with national leadership and stakeholders of the nuclear industry to better understand cyberthreats and to develop good practices that enhance computer security. National training courses, Dudenhoeffer said, are some of the most valuable activities that the IAEA conducts in computer security.

"In physical protection, you can see what you're protecting and visualize probable attack scenarios," Dudenhoeffer said. "But in cyberspace, criminals have many more targets including those not at the facility; you could even be attacked at home. We must learn to think like the criminals to better understand how to protect against cyberattacks wherever we are."