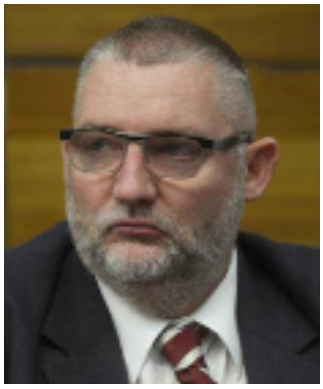
Editorial

Welcome to another edition of the Romanian Journal for Cyber Security. We strive to develop and improve this publication as a product around which to build a community of experts that can tackle, through debate and the sharing of knowledge, some of the most important problems of our time. As we speak, and in full pandemic, the cyber security issue has never been more current or more serious. We have seen with the Solarwinds attacks that countries and businesses are increasingly vulnerable to supply chain attacks and business process software intrusions. When the attack on Solarwinds' Orion network management product was first announced, it was estimated that the intrusion had been going on for months without having been detected. This may have seemed shocking to some, but we know from various studies, including those by Marsh & McLennan for the World Economic Forum and many others, that the mean dwell time, the period between intrusion and detection, is, on average, around 100 days, and for Europe it was particularly worse just a few short years ago. It will take time for the new legislation and investment into cyber security and security culture to make their marks.

In the meantime, we live in an ever more competitive and challenging security environment, in which our dependency on cyber systems grows much more rapidly than our capacity to manage and mitigate the security implications. Articles in this and other issues of ROCYS have highlighted the race between consumer product companies, hackers and security decision makers to see who can keep ahead of what the others are doing. The world of the Internet of Things is a world of ubiquitous communication and danger, in which the interactions between previously isolated or non-digitized systems create new risks, vulnerabilities and threats in patterns and behaviors which were not obvious or immediately apparent to the security experts. This is what the growing complexity of the world leads us to, and what we must prepare to face as the price of the race towards new economic efficiencies, new products and new capabilities.

The Solarwinds debacle was instructive in many different ways, which I hope that future contributors will address in the pages of ROCYS in due course. Firstly, there was significant evidence that led the Americans towards concluding that Russia was behind the attack as a means of gaining access to US government systems and networks. This is par for the course in the murky world of hybrid warfare, where everybody keeps tabs on everybody else. It was the



Dr. Adrian Victor VEVERA
Founding Editor in Chief,
General Director,
ICI Bucharest

willingness to directly and publicly attribute the attack to Russia that raises eyebrows concerning the future course of cyber attacks, where the difficulty in attribution prevents retaliation or criminal prosecution of perpetrators.

Secondly, the technological aspects, and the marriage between commerce and security are all very interesting, but the Solarwinds attack hinged at least partially on an intern using the password solarwinds123 for a server. This points in an important direction, both for Solarwinds and the entities who were hacked through it but might as well have been hacked on their own – security culture matters! Not just the quality of experts and cyber warriors one employs, but the basic knowledge and habits of rank-and-file employees, from the CEO to the lowliest intern. Remember John Podesta's accusation that the Russians had hacked the Democratic National Convention's servers during the 2016 election to steal data and help Trump? It may be true, but the subsequent revelation that his password has been "p@ssword" certainly lowers the bar for hacking the DNC to anyone with a basic knowledge of such issues.

Thirdly, the economic incentive for cybercrime and the diversity of capable actors, both individual and collective, local and transnational, have become so great that rival states may take a backseat in hacking attempts to decrease the likelihood of true attribution, or even act as passive beneficiaries of cybercrime, as hackers sell or release important information that becomes actionable intelligence, or they undermine the general security of institutions and networks.

Fourthly, we have not been speaking enough of the major change to the cybersecurity landscape – the explosive growth in work-from-home arrangements because of the pandemic. Exploiting unsecure home networks to infiltrate more secure business networks has probably already become a key development, it will just take a while for it to be noticed, quantified and for it to make it in the specialty studies.

There is never a dull moment in cybersecurity. I am glad that you are here with us to discuss these issues and stay ahead of the great changes underway.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!