A World of IN-Security

Ramsés Gallego

CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt

Security, Risk & Governance International Director, Micro Focus

COVID-19 is showing us how fragile our world is and how rapidly our society can be at a halt. With ease. Many industries have been obliged to stop producing goods and have kept their employees at home… because of a virus, an external threat that could have been mapped, defined, considered in the first place but without a cure… like a zero-day attack.

We are living through difficult times that takes us, once again, to the stages of planning, designing, envisioning and executing the right protection measures, the appropriate controls, the very much needed processes and procedures to bring back a healthy environment for our communities to thrive and shine again. And the digital dimension is no different from the physical world. It is instrumental that we understand the (ever expanding) threat landscape, that we comprehend the different angles of the surface of attack so that we, together, protect supply chains and the different industries in which our society is built upon.

That approach requires to check different dimensions. As it happens with viruses, where one needs to check its origin, its path, its velocity of spreading, its capabilities of muting into another version of the threat,… it is fundamental that we check, in the digital field, who has access to what, how an information is threatened by a potential leak, why some sensible application is not hardened when uploaded to the cloud. All this requires the right mindset, a robust and solid approach to security that moves away from tactical security and fully embraces security from the inside out.

There has never been a better time like this one to consider a security that is not tactical in nature but strategically at its core. There has never been an epoch so critical where the right questions are presented to the right people at the right time. And that includes adapting and adopting mitigation strategies to reduce the exposure factor of a company, to minimize the risk of impacting the VaR (Value at Risk) with attacks that not only come once (Single Loss Expectancy, SLE) but many times (Annualized Loss Expectancy, ALE). The strategic approach that will enable the conversation not just about 'a security platform' but 'a security ecosystem'. Since an ecosystem can be both systematic and systemic. Yes. Systematic because the appropriate processes and procedures will bring orchestration of security, automation of protection. It can be systematic in its way to self-protection and providing automated responses in context with the attack happening; systematic through the intensive use of (unsupervised) Machine Learning. And an ecosystem can also be systemic because it belongs to an 'everything', a whole system, it is part of something bigger… and part of the overarching equation of protection and defense. An ecosystem brings value in minute one -if properly defined- since it can be industrialized (systematic) and is part of something bigger (systemic) such as the governance of the enterprise IT, enterprise risk management or any other name that we want to consider for the holy discipline of protection and defense.

An ecosystem cannot develop without taking into account each and every angle of itself. In the digital arena these are identities, data and applications. People gathering information, customers using data, users governing their digital personas,… Identities – Data – Applications live at the core of any security ecosystem that aspire to be comprehensive, end-to-end, robust, solid,…

We feel honored at Micro Focus to have that approach to the way we live -and breathe- security, risk and governance. We applaud any initiative that is targeted to fortify applications, to encrypt data -wherever it lives- and to ensure that someone is who they say they are. It is the epitome of an enhanced security posture that understand the three very pillars of every company on the planet: Identities, Data and Applications. We feel that no ecosystem can survive only embracing one or two of those dimensions.

These are times to hold to the truth of a security ecosystem. These are the times to beat viruses and any other type of threat. These are the times to move away from insecurity and consider security from the inside out. These are the times to be IN Security. This is how we win. Period.