Security is Community

Myth

Cybersecurity is a battlefield, form of insurance, or a luxury item.

Truth

Security is community.

Introduction

This document is intended to address a common misconception that cybersecurity is a state of war, insurance policy, or luxury.

We deem these notions to be inaccurate and aim to shed light on this subject in the following paper.

Explication

Cybersecurity is a complex and expansive realm of expertise that directly impacts nearly every industry. An effective way to view cybersecurity is like herd immunity. The goal is to protect as many systems as possible, because unprotected systems further fuel cyber criminals as well as affect the economy and productivity in which everyone is a part of. Security is community and requires us all to *work together* to set the bar high, so criminals seek better use of their time.

The first fallacy we would like to discuss is the cybersecurity as a state of war notion. We often hear references to security as a battlefield between security professionals and rival criminals. While skirmishes involving governments, corporations, and other collectives exist and have important implications on common well-being, they represent just one piece of the greater landscape. Security requires collaborations and contributions by many different parties worldwide with varying skillsets and motivations. Most importantly, the security field needs public involvement, attention, and education. The us-versus-them wartime narrative is simply not compelling enough to inspire the masses into action, and this inspiration should be a primary objective of anyone who is passionate about protecting the systems embedded in our lives.

Though fear will always be leveraged by some to generate sales demand, the truth is that there is no need for anyone today to live in fear of cyber attacks. It is far more beneficial to society for everyone to accept the reality that one's computing devices will likely get attacked at some point in their lifetimes. From that mindset, an important question can be asked: if and when the system gets compromised, how much will it cost the owner in

terms of time, money, and information leakage? There are leading embedded security products available that assume the attacker already has root access to the target. It is acceptance of the inevitable that puts system owners in a powerful position.

The second fallacy to discuss is the idea of cybersecurity as a form of insurance. The issue with this concept is that if security is insurance, then that makes the system owner a policyholder and implies that they will always need an insurer. No bueno. While often times it is pertinent to buy security products and services from appropriate sources, the system owner must understand how important their own role is in protecting the asset. The owner is not merely a source of funding nor is the security field just a black hole to toss money into.

System owners need to oversee the system through its lifetime and ensure that the system remains fortified as technology evolves. Protecting the world's devices requires responsible parties to become educated and develop necessary habits. That is why it is a QVLx objective to *empower* as well as protect, and this mantra was a lodestar in the development of the Salvum® Security Engine. Various QVLx training options are also available

to embue system owners with the arcane knowledge to maintain a system as well as make informed decisions on additional specialist services needed. Less money will be spent this way.

The third and last fallacy to explore is cybersecurity as a luxury item. If securing a system costs so much that only a small fraction of the world's devices can afford protection, then the mission of security providers has failed and the societies in which we are all a part of will remain unnecessarily vulnerable. Security is community and a very large dedicated community at that. By leveraging worldwide researchers, commercial product providers and open-source contributors in the security field, protecting systems can be made cost-effective enough to be accessible to everyone. Salvum is a testament to this fact.

What misconceptions around cybersecurity have in common is that they misconvey the world as being smaller than it is. We must not forget the work of so many people to make security what it is today. With their help and by educating the public, societies can build strong unified perimeters that are not worth the effort to breach. QVLx can't operate without community and hopefully every embedded system owner will follow our lead.

About QVLx

QVLx is a disruptive supplier of critical embedded systems expertise, products, and innovation. Our company helps customers develop complex, robust, and elegant solutions to meet their most demanding requirements in excellence.

QVLx is headquartered in Huntsville, Alabama.

For more information, visit qvlx.com