All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Why can't we make any of the systems we use secure from remote attack?

We see lots of different approaches to building more secure systems and software, but none of them seem to work. We see massive movement toward and spending on detection and response, but detection still lags, and response is painfully too late in case after case. But have you ever asked yourself why we ca't build systems so they can't be attacked from afar?

Nobody can answer this, because...

It turns out there is a reason nobody can answer this question. It's because the answer is that we can build systems that are secure from remote exploitation. While it was often thought to be too hard because it takes time and is expensive to do, and of course perfection is unlikely to be reached in any human endeavor, and nothing lasts forever, and the best defense is a good offense, none of these are in fact true when it comes to computer security.

Try harder!

It turns out we can build quite secure systems against large classes of threat actors, but we have to decide we want to. The fundamental problem we face is not the inability to do it, but the desire to be better, faster, cheaper, but not more secure. There is a tradeoff between doing it fast and doing it right. The 90% solution fails every time in computer security because we have lots of folks trying to attack, and few trying to defend. The attacker gets lots and lots of tries, while the defender puts something out there and waits for it to fail.

How many 9's do you need?

If we want, we can build and operate systems with 99.9999999% security solutions, and we can add more 9s if we want to. But 9's cost money, and it's a reasonable assumption that every additional 9 costs more than the previous one. Until recently, the cost of failure was not very high. We had plenty of warning, certainly 30 years or more of it for every attack methodology in widespread use today. Despite the warnings, we increased dependency every year, increased the value of attack every year, and decreased the spending for preventive defense per unit every year. We are quite simply reaping what we sowed.

How do we escape?

We dug ourselves into a hole as a society for 30+ years, and good advice would be to stop digging. But we seem to be unable to stop. We continue to increase dependency, but we don't have to. We continue to increase the value of attack, but we don't have to. We continue to go as cheap as we can on prevention to the point where we have created an industry focused on it, and we appear unable to break free of this habit as well. The escape is decision-makers no longer taking what is offered, but demanding what is needed – and paying for it.

Summary:

It took 30+ years to dig the hole, and filling it in will take a while. We need to start filling in the hole and spend the money to get what we need while demanding it from our vendors.

