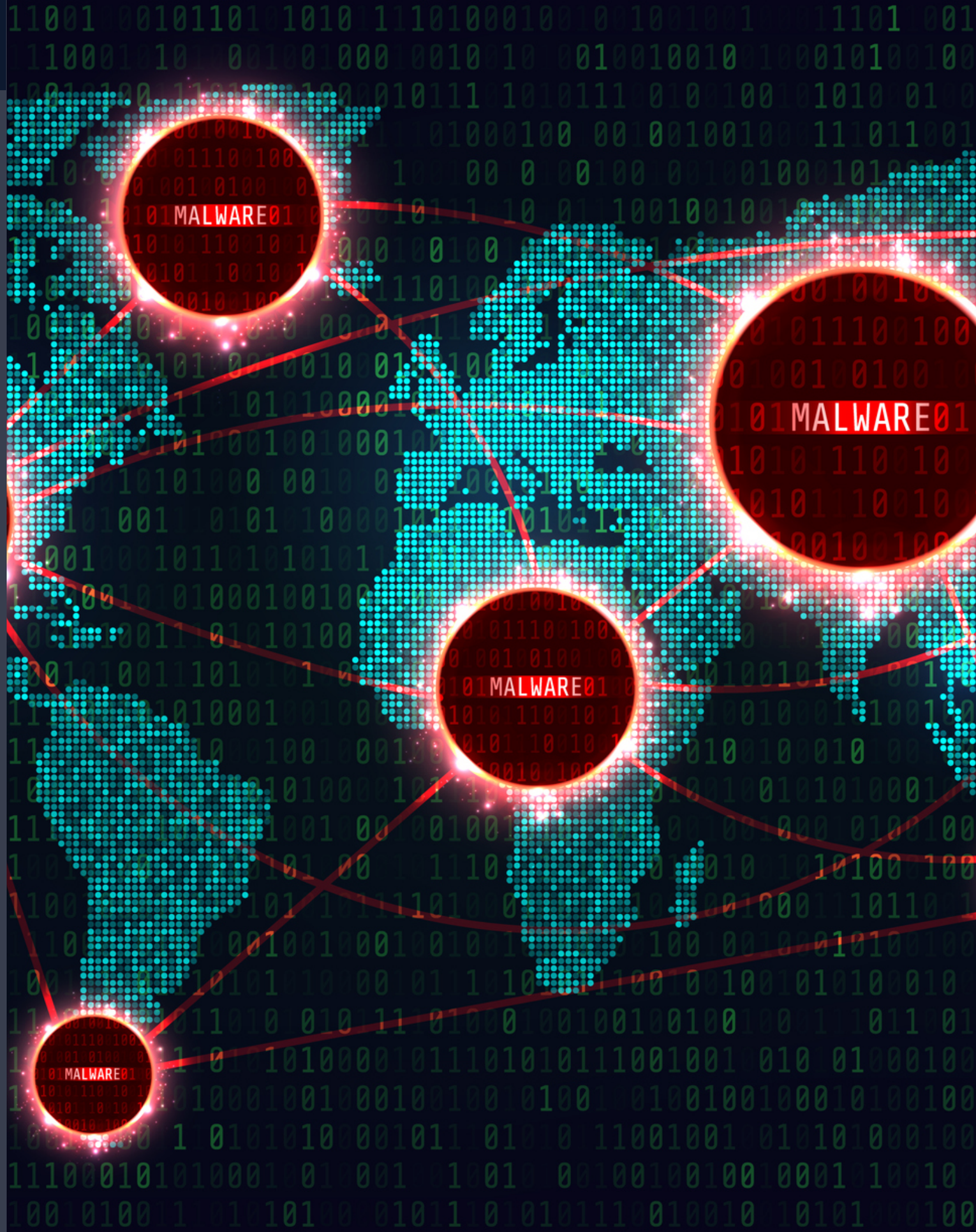
TICKWALL
SECURING ACCESS FROM OUTSIDE

Monotek d.o.o.

TICKWALL, SECURING ACCESS FROM OUTSIDE

A brief on how to reduce your external attack surface.



TICKWALL
SECURING ACCESS FROM OUTSIDE

The problem.

WHY?

- **No matter what you do, your assets have vulnerabilities that are already discovered, or will be in the future.**
- **You can never patch the vulnerabilities as quickly as somebody will be able to exploit them.**
- **A hacker never relies on access when you are behind the computer, but searches for his own way in. Full time, any time.**
- **By closing access for the world you have effectively also closed access for your employees as well, until now.**

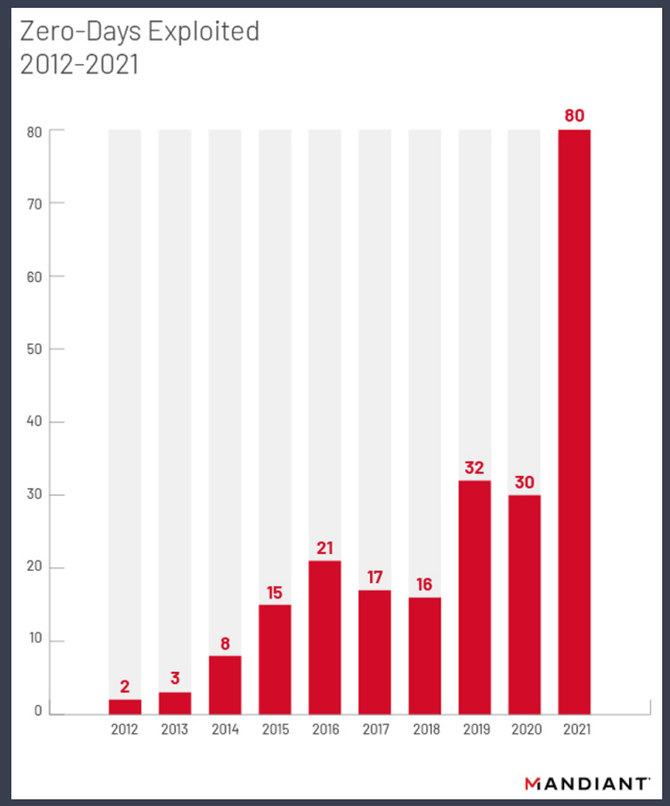
The problem is as old as the cyber world itself. How to share a service to the world, but not allow it to be exploited. A hacker always goes down the fundamentals and tries to see if the developer of your application remembers the fundamentals of secure coding and software design.

However in today's world, security is something companies may start to afford within the design phase usually and only after they have been breached or publicly exposed for having poor Quality Assurance or development procedures.

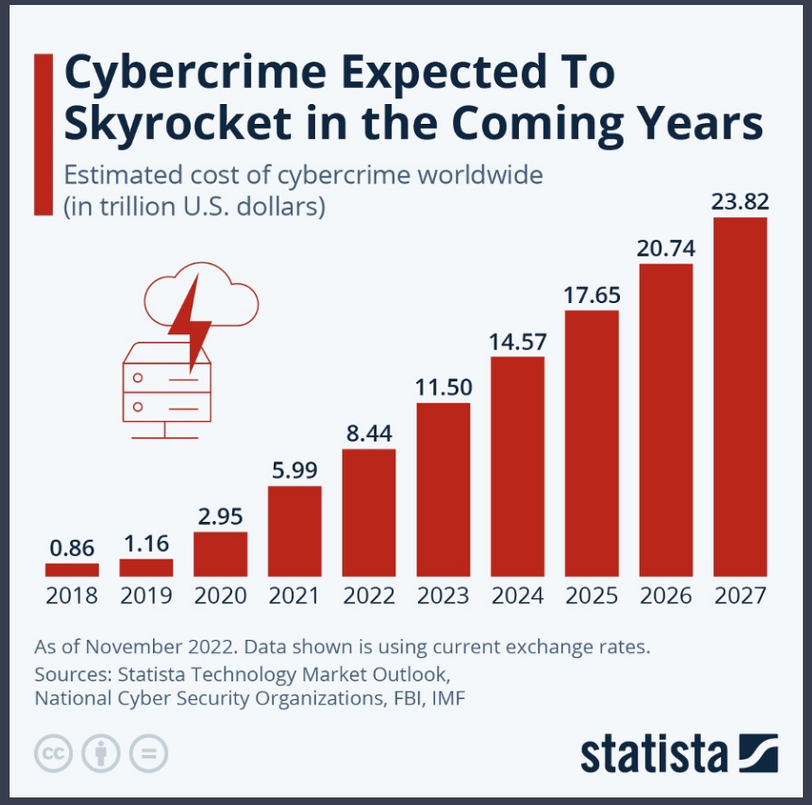
This means, the majority of software companies focus on market demand, feature rich solutions that solve problems for their customers, and tend to see secure coding, bug hunting, code analysis and penetration testing as unnecessary costs and release delays, for which there is no commercially viable reason, until it becomes one.

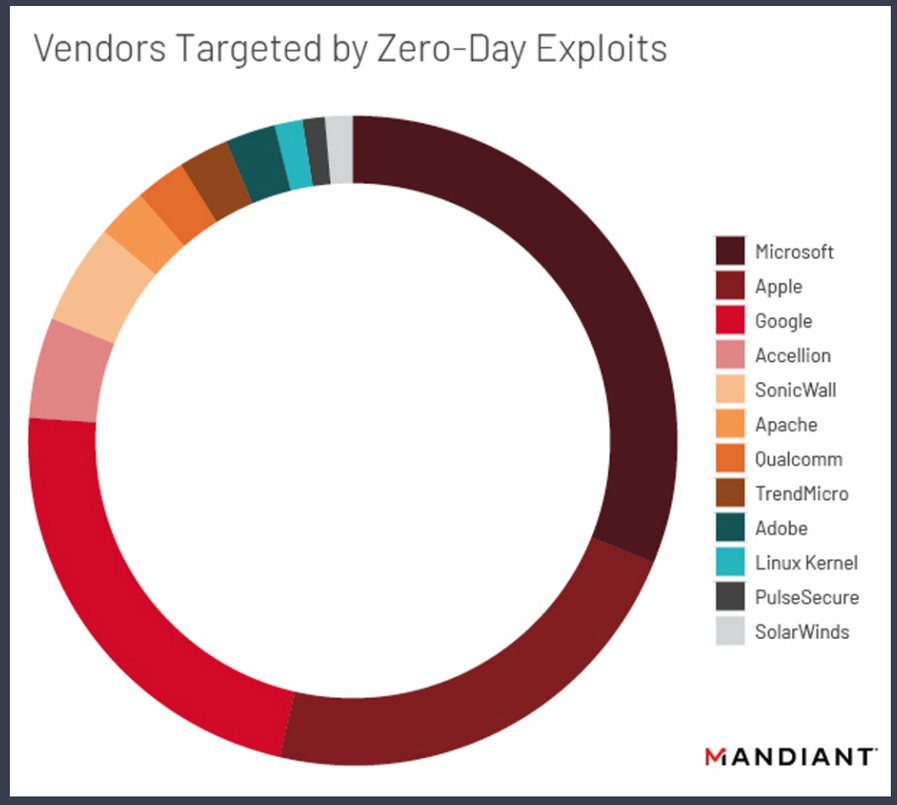
In all honesty, we will probably never get this right. We will probably never get software that is secure by design the first time. We will always have necessities for visionary solutions that are here and now, and solve our problems or make our profits, but fail the resilience of so much secure by design investments that happen in mature organisations or products over time.

We understand this fact, and we are here to help.



As you can see, there are no safe vendors and no safe prospects for the future. The staff you have today will probably be the staff you will have tomorrow. What organisations need to do today is pretty much similar to what they will have to do tomorrow. Patch, maintain, evaluate, service, implement and patch again. And be vigorous about it, and even if you do get it right, there will be exploited systems that the vendor hasn't published a patch yet for. So what you can do then is close it down and keep it down, until somebody fixes the thing. But can you really do that (like in the case of PrintNightmare), and is that the only way to reduce your vulnerable attack surface?





TICKWALL
SECURING ACCESS FROM OUTSIDE

Understanding the issue.

WHAT

- **Patching fixes past problems, it doesn't fix the unknowns of today or tomorrow.**
- **Patching doesn't protect against social engineering.**
- **Even if you don't believe in security by obscurity. Somebody not knowing your secrets or truths, may not be able to exploit them.**
- **Why give everyone an opportunity, narrow the field down, become invisible to the world with your infrastructure.**

By no means do we discourage patching, awareness training, penetration testing, and buying secure solutions from the start, and of course encourage all other security mandatories an organisation needs to perform in order to stay sanitised, but we feel the fight is unfair and we might be able to even out the odds in a simple but a different approach.

To address this issue, we need to reinvent a few truths, so the problem becomes more abstract, and the solution more obvious..

So let's say your organisation has infrastructure, your 10,000 employees travel all the time to meet strict customers demands and of course they need access to everything, and anything in your back-office. The natural way to provide this is to enable access to your services from the internet, and as soon as your employees are online (from branch offices, hotels, airports, airplanes, or from home) they can connect to your service. The whole internet theoretically has **4,294,967,296** IP addresses that you have allowed access from. So for **10,000** employees that hardly seems fair.

TICKWALL
SECURING ACCESS FROM OUTSIDE

The solution?

WHAT IF

- **You don’t need to allow the whole internet, but can create a bubble within?**
- **You can be late on your patches, and not risk an immediate, automated shut down of your services.**
- **You could lock down your infrastructure to only your employees, wherever they are.**
- **This could also be applicable to your customers, your machines, your products, and for your whole service supply chain.**

What if we could provide your firewall with a list of the exact **10,000** IPs your **10,000** employees are using right now, and refresh that list as quickly as 60 seconds (some cases even less). With that IP list, you could lock down your services only to your employees, and close off access for the rest of the world.

Would that reduce the risk your infrastructure is facing? Would you still be a sitting duck, waiting for an exploit to happen, or would be under stress if the patches for the vulnerabilities, exploited in the wild will come in time for you to fix them. Or would you have to make decisions to take down those now vulnerable services and know it will hurt your business until they are back up.

Now if we look at the fundamentals, the numbers do not lie. Take it up with your risk department, do the calculations and send us an e-mail. We will gladly provide a trial, and help you secure your internet facing infrastructure, be it on-premise or in the cloud, be it a vpn connection point, an e-mail server, a web server farm, or a highly scalable proprietary service, if it’s accessible from the internet, and less than **4,294,967,296** IP’s need access, we can help you.

info@tickwall.com

tickwall.com