SECURING THE MAINFRAME: WHAT ARE YOUR PRIORITIES?

It never rains but it pours. In other words, when one bad thing happens, other bad things often follow in its wake, sometimes to excess. The SolarWinds Orion supply chain compromise was yet another in a seemingly endless stream of hacks and attacks. Stormy times.

It's also been said that the best time to fix a leaky roof is when the sun is shining – ideally before the bad weather hits and does its damage. I'm mixing my water metaphors, but if you're in the fortunate position that the rising tide of cybercrime hasn't breached your own organization yet, there's no time like the present to check your defenses, confirm they are intact, and plug any gaps.

Here, in no particular order, are some the issues and activities that should be on the current priority list of mainframe teams, security experts, CISOs and, indeed, CEOs.

The most recent BMC Annual Mainframe Survey revealed that today's mainframe is consolidated as a core element of the modern digital enterprise; a hub for innovation, helping organizations to create and deliver the "intuitive, customer-centric digital experiences" of tomorrow. The other big takeaway from the survey was that security and compliance are now the top mainframe priorities.

These increased digital demands will require new and enhanced processes. For example, with calls to update applications on the mainframe faster and more efficiently, we'll see further developments in DevOps. As a BMC colleague wrote recently, "With the right procedures, tooling, education, culture shift and mind set, the business-critical applications that currently run on mainframes can easily be integrated into a DevOps operation." This reflects the continued prevalence and power of the mainframe: it's fast, scalable, resilient, securable, flexible and available, able to "handle the workload of thousands of x86 servers for a fraction of the TCO and manpower."

But the usual storm clouds are gathering, and threaten to rain on our parade. As more people

become interested in mainframe tech, more information appears on the web – and how it can be hacked. The only thing stopping a tsunami of attacks right now is the platform itself: it's still too expensive and tightly controlled to be accessed, taken apart and reverse engineered. But that will change. So CISOs need to focus on ramping up their defenses: from access rights, password policies and insecure applications to overprivileged users, the threat of unencrypted communications and more.

This means taking more active steps to embed a 'Zero Trust' culture. We live in a mainframe world where READ access is so often the norm, when default access should actually be NONE. We should be applying the principle of least privilege (PoLP). Organizations need to up their game in terms of threat detection and response capabilities, moving to Extended Detection and Response (XDR). The threat landscape is continuing to shift, evolve and mutate – yes, like a virus. Harnessing automation, AI and machine learning through XDR may be our salvation; a shot in the arm for mainframe security.

To support these and other initiatives, another trend is increased demand for mainframe services, including security assessments and pen testing. With the pandemic and home working accelerating digital transformation in so many organizations, new processes and security challenges have emerged. With a persistent skills and resource shortage, engaging external experts makes sense: extra people for specialist projects, keeping the lights on, or improving your security posture.

In summary, I think three main drivers will help to shape our priorities in the months and years ahead. First, the huge additional demand for employees to work remotely and access their corporate systems from home, requiring new processes and creating new threats. Second, continuing complacency and the mistaken belief that the mainframe is inherently secure: it isn't, and we need to plan and deliver a Zero Trust approach. And third, the increasing threats posed in a connected world by a supply-chain attack. The bad actors don't need to get to your production systems, which may be tightly protected. They can instead target the systems of a supplier or someone else in your supply chain. Securing the supply chain will be another priority.

We *can* do more, and the tools and expertise are already out there. We need better analytics, automation and adaptability, drawing on external expertise if needed, all underpinned by informed governance and the latest policy-based approaches. It won't always be plain sailing but it's the only way we can start to roll back the tide. Nobody wants to go under.