SOLVING THE SECURITY RISK YOUR CISO DOESN'T KNOW ABOUT

What do you do when your car breaks down? A major home repair is needed? What if you have a toothache? Some of us might try a DIY fix, but odds are in most of these cases (especially the latter) you look to the services of an expert. Security is no different with security services now accounting for more and more of IT budgets.

The use of managed services has grown in the last few years. A big driver is that managing risk is more and more at the top of the CIO/CISO list of challenges but staffing and expertise are in short supply. Often, I find CISOs who have put Data protection, Incident response, EDR, endpoint security and infrastructure management services on their list for consideration to implement better security standards. My first follow-up question is usually "And what about your Mainframe? Who are you engaging to harden security and protect the data that lives there?" I'm usually met with a puzzled face. The mainframe has been thought of as the relatively secure box that lives somewhere in the infrastructure and isn't tied to the corporate security initiatives. However, as a connected device with sensitive data that IS vulnerable it must be secured just like any other device.

The reality is that despite the confidence many have in the security of the mainframe, it can be compromised in as little as 6 minutes. That's right, I said 6 minutes. And mainframes have an average of over 100 high risk vulnerabilities on them. How do I know that? I'm the guy that achieved that 6 minute mark and performed the pentests that found those vulnerabilities.

Apart from a better security posture, why else is securing the mainframe important? In the annual BMC Mainframe survey, 92% of respondents to the survey reported being audited at least every two years. 77% have been subject to a finding or potential breach. Simply put, without knowing how

vulnerable your mainframe might be, you are highly likely to find out in the next couple of years and if you're like the majority of people, it probably won't be reassuring news. Not only that, but Forrester Research found that mainframe use is growing with 50% of respondents saying they plan to GROW their use of mainframe over the next two years. More use = more data = more risk for companies.

So what is the solution for the CISO or Security Operations person who doesn't want to take a DIY approach to securing the mainframe? Services provided by experts, tailored to the needs of the company. Do you want to know if you're in the 100+ vulnerability club? Consider a security assessment. Are you lacking the staff or expertise to keep the mainframe secure or just perform routine maintenance? Maybe security-as-a-service, a managed mainframe infrastructure service, ad-hoc skill services or a expertise on-demand can help address the gap?

To learn more about how mainframe services can help you better secure, maintain and address the staffing and skills challenges you're facing, watch this webcast to learn more about where BMC Mainframe Services by RSM Partners can help!