BIZCOMMUNITY

20% of companies in SA have no cybersecurity plans for holidays or weekends, study finds

Cybereason, a cybersecurity technology company, has published a global study of 1,200+ security professionals at organisations that have previously suffered a successful ransomware attack on a holiday or weekend. The report, titled *Organizations at Risk: Ransomware Attackers Don't Take Holidays*, highlights the disconnect between perceived threat and preparedness that results in longer incident response and recovery cycles.

Lior Div, CEO & co-founder of Cybereason | image supplied

The study found that most security professionals expressed high concern about imminent ransomware attacks, yet nearly half felt they do not have the right tools in place to manage it.

In addition, nearly a quarter (24%) still do not have specific contingencies in place to assure a prompt response during weekend and holiday periods despite having already been the victim of a ransomware attack.

Similarly, in South Africa, the study found that 20% of companies have no security plans for holidays or weekends.

The findings highlight a disconnect between the risk ransomware poses to organisations during these off-hour periods and their preparedness to respond moving into the holiday season.

Organisational impact

The lack of preparedness for ransomware attacks on weekends and holidays has a significant impact on victim organisations, with 60% of respondents saying it resulted in longer periods to assess the scope of an attack, 50% reporting

they required more time to mount an effective response, 33% indicating they required a longer period to fully recover from the attack.

In South Africa, 38% said it would take longer to stop if the attack took place on a weekend or holiday. More concerning is that 84% of respondents said they were intoxicated on the job responding to an attack on a holiday or weekend.

This research validates the assumption that it takes longer to assess, mitigate, remediate and recover from a ransomware attack over a holiday or weekend.

Technology issues

Another indicator of the disconnect between the perceived risk and preparedness includes the fact that although 89% said they are concerned about attacks during weekend and holiday periods, 49% said the ransomware attack against their organisation was successful because they did not have the right security solutions in place.

Kaseya ransomware attack: 80% of companies that pay are hit a second time

Lior Div 6 Jul 2021

Just 67% of organisations had a NextGen Antivirus (Ngav) solution deployed at the time of the attack, 46% had a traditional signature-based antivirus (AV) in place, and only 36% had an Endpoint Detection and Response (EDR) solution in place.

The human element

On the human side of the equation, 86% of respondents indicated they have missed a holiday or weekend activity because of a ransomware attack, a situation that can factor into employee job satisfaction and potential burnout.

One surprising finding in the study included 70% of respondents confessing that they have been intoxicated while responding to a ransomware attack during a weekend or holiday, a risk factor that many organisations may not have accounted for in their incident response planning.

Retail and transportation: industries at risk

As we enter the holiday season, the retail and transportation sectors present high-value targets for ransomware attackers given the potential for disruption and lost revenue that increase incentives for victims to pay higher ransom demands.

Key findings for these sectors include nearly 70% in both Retail and Transportation who said previous ransomware attack was successful because they did not have the right security solutions in place and 24% who said their organisations still do

not have a specific contingency plan to address the risk from weekend and holiday attacks despite previously having been a victim.

“Ransomware attackers don’t take time off for holidays. The most disruptive ransomware attacks in 2021 have occurred over weekends and during major holidays when attackers know they have the advantage over targeted organisations,” says the chief executive officer and co-founder of Cybereason, Lior Div.

“This research proves out the fact that organisations are not adequately prepared and need to take additional steps to assure they have the right people, processes and technologies in place so they can effectively respond to ransomware attacks and protect their critical assets,” he adds.