RESILIENCE & RECOVERY: CRITICAL IN THE FIGHT AGAINST RISING RANSOMWARE ATTACKS

Team8 – Global venture group
10 Mar 2021

In a world where digital infrastructure is now synonymous with business-critical infrastructure, cybersecurity cannot afford to stop at "protect, detect, and respond". Recovery can no longer be an afterthought - it must become a core tenet of risk mitigation and business continuity. Any sound security strategy necessitates capabilities that enable rapid recovery from degradation, disruption, or denial of access to enterprise systems or data, and swift reconstitution of assets and capabilities.

Drivers

Ransomware and destructive malware are on the rise. In 2015, Kaspersky reported that ransomware was doubling every year. However, Bitdefender found that 2020 brought a seven-fold rise compared to the previous year.[1] Opportunistic attackers are taking advantage of the surge in digitization and new security challenges during COVID-19 which, in combination, make organizations more vulnerable to cyber threats. Overall, the average severity of insurance claims reported by policyholders jumped by 65% from 2019 to 2020, driven largely by the rising costs of ransomware as cybercriminals ask for higher amounts of money and increasingly threaten to release stolen data publicly unless the ransom is paid.[2] An October 2020 Treasury directive, aimed at stymying ransom payments by threatening enterprises who pay with sanctions, could either provide a much needed headwind against this alarming trend or put enterprise leaders, staring down the barrel of a severe ransomware attack, between a rock and a hard place.[3] As enterprises adjust to the business disruptions caused by the pandemic, disaster recovery and business continuity plans are critical. This isn't only a matter of cybersecurity but also of operational resiliency. Any network outage or other disruption to infrastructure can put companies on the sidelines or entirely out of business for months. For many companies, there is no "Plan B" and in today's climate that is a particularly dangerous position in which to be. Even the best security teams will succumb to attacks and knowing how to continue to offer services to customers is essential.

Impact - Ransomware is just one example of the damage threat actors are causing businesses. Systems can be modified, data stolen, and infrastructure brought down for a variety of reasons. Companies need a reboot plan designed for the digital age, to build resiliency and accelerate recovery from damage or disruption.

Solutions - Backup and Disaster Recovery, Application Performance Monitoring, Self-Healing Systems, Cyber Exercise Facilitation, Cyber Ranges.

Perspectives:

- **Defender's Perspective** - *"We've made great improvements to our cyber posture that have pushed down the probability of an attack. However, the magnitude of impact has stayed the same or risen because we're more digitally reliant. What COVID-19 has shown us is that low probability, high impact events can happen. Defence is still a core component of any good strategy, but there is an increasing importance for enterprises to quickly reboot in the event of digital catastrophes." - Paul Branley, Director, Strategy, Innovation & Testing at Lloyds Banking Group.*

- **Team8's Attacker Perspective** - *Ransomware attacks have evolved beyond holding production and productivity hostage. Improvements in Business Continuity Plan (BCP) and resilience have pushed attackers to make additional threats - publishing data if a payment isn't made. This creates a problem for organizations that want to minimize the effects of ransomware by introducing resilience. As systems become more resilient, this two-pronged approach [used by attackers] will proliferate. The latest US Treasury directive threatening prosecution or sanctions to enterprises who pay off certain ransoms could alter this dynamic by pushing attackers to find other ways to monetize their ransom.*

In our next blog, we will cover Shift-Left.

The views expressed in this blog are those of Team8, any reference to "we" should be considered the view of Team8 and not necessarily those of WisdomTree Europe.

Team8 is a global venture group with deep domain expertise that creates companies and invests in companies specializing in enterprise technology, cybersecurity, and fintech. Leveraging an in-house, multi-disciplinary team of company-builders integrated with a dedicated community of C-level executives and thought leaders, Team8's model is designed to outline big problems, ideate solutions, and help accelerate success through technology, market fit and talent acquisition. For further information, visit ***www.team8.vc****.*

Sources

[1] https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

[2] https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf

[3] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Related blogs

+ Introducing cybersecurity, the megatrend of the 2020s
+ Cloud security: A necessary component in digital transition planning
+ Security of Things: Dealing properly with the explosion of connected devices
+ Perimeterless world: Networks are becoming less tied to physical locations
+ Privacy & Digital Trust: 2010' s were about Data Collection, 2020' s will be about Data Protection

Related products

+ WCBR - WisdomTree Cybersecurity UCITS ETF - USD Acc

View the online version of this article here.

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

The application of regulations and tax laws can often lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.