optec

Preventing Ransomware in SMBs

Protection begins by knowing how ransomware works

Though ransomware poses a threat to all organisations, small and medium businesses (SMBs) are particularly vulnerable. In fact, more than 70% of ransomware attacks in 2018 targeted small businesses. The reason: many SMBs lack the internal resources, knowledge or security budget to confidently prevent ransomware and deal with the ramifications of a successful attack. To fight ransomware, today's businesses require a comprehensive security solution that is simple, straight-forward and affordable.

Hackers Are Attacking SMBs with Ransomware

Ransomware is a type of cyberattack where hackers gain access to a organisation's network - usually through malicious email – and demand payment for the release of the organisation's data. While large organisations can sometimes absorb ransom demands, for SMBs, a ransomware attack can be catastrophic. For many SMBs, the loss of critical business cycles and revenues from systems that are grounded far outweigh the price of the ransom itself.

Gaps in Security Threaten Smaller Businesses

The need for speed and agility has led many organisations to adopt new technologies, such as Software-as-a-Service (SaaS), public cloud, and other omnichannel customer engagement tools. While these tools bring convenience and flexibility, they also create security vulnerabilities. When administrators are unable to understand how applications are using data and how users are accessing them, it makes it easier for even basic threats to get past defences, especially when those defences aren't effectively communicating.

For many SMBs, security is a mishmash of different solutions. Each product has its own version of policies and rules that don't mesh with other products without customisation or additional third-party technology to translate from one device to another. This makes it easy for bad actors to exploit gaping security gaps. And as the world shifts to more users engaging outside the traditional perimeter, businesses can't expect ransomware attacks to wane. The vulnerability factors, relative ease of implementation, and high-profit potential for bad actors only mean the frequency of attacks with continue to rise.

By 2021, there will be a ransomware attack every 11 seconds.

How Malicious Emails Circumvent Security

- **Email attachments:** Attackers use advanced technology that's designed to evade security. Without a way to analyse the attachment, organisations have no indication of the threat.
- **URLs embedded in email:** Sites that look legitimate are often blindly clicked. Many organisations are unable to analyse embedded links, nor can they identify known malicious sites.

How Ransomware Attacks

Step 1
Email
A user receives a malicious email that appears to be legitimate with a link.

Step 2
User Clicks
Once the user clicks the link, the attack is launched.

Step 3
Hunts Network
The malware then hunts for key data and folders, and can disable backup and recovery.

Step 4
Encrypts
The malware establishes command and begins to encrypt files.

Step 5
Lateral Movement
Without network segmentation, the malware spreads laterally.

SMBs Need a New Approach in the Fight Against Ransomware

SMBs need to be ahead of the curve when it comes to taking precautions against ransomware threats. In this fight, prevention is the best defense. When considering an approach to protecting against ransomware, SMBs should make sure their solution is:

94%
of cybercriminals in general leverage email to begin their attacks.

- **Effective and Comprehensive:** For a solution to be truly effective, it must provide broad coverage. Ransomware only needs a small opening to be effective, so it's critical to plug every hole in security coverage.

- **Easy to Use and Affordable:** Many SMB security teams are focused on many tasks, perhaps lacking specific malware prevention expertise. A solution needs to be simple, straightforward, and affordable - one that gives the organisation the level of protection they need without the burden of overstretched resources and/or budgets.

- **Reputable and Lasting:** SMBs must be smart about their investments. Buying something only to throw it away along with the solution experience when its capabilities can't scale as they mature just isn't a smart option. Hackers are continuously evolving, so should cybersecurity capabilities of SMBs. Their security providers should be able to show long-term ROI as part of the proposed investment.

Fortinet Delivers Comprehensive Protection Against Ransomware

The Fortinet Security Fabric brings end-to-end security to SMBs to prevent ransomware across all points of entry. Powered by intelligence from FortiGuard Labs, Fortinet combines market-leading prevention, detection and mitigation with top-rated threat intelligence to combat today's most advanced threats.

FortiMail Prevents Phishing & Other Email-Initiated Attacks
Available as a SaaS offering or on-premises device, FortiMail brings powerful anti-spam and anti-malware capabilities to organisations to stop unwanted bulk emails, phishing attempts, and other business email compromise techniques.

Security-Driven Networking Prevents Malicious Files and Communications on the Network
The Fortinet FortiGate next-generation firewall (NGFW) is the most widely deployed NGFW on the market and ensures malicious actions and communications crossing the perimeter are blocked, such as when a user accidentally arrives at a malicious website and a drive-by download attack ensues. Administrators gain visibility over how applications are interacting with data, users, and the devices with out-of-the-box reporting and the ability to easily control these activities to better protect the business.

FortiClient and FortiEDR Stop Attacks at the Endpoint
FortiClient strengthens endpoint security through integrated visibility, control, and proactive defence. With the ability to discover, monitor, and assess endpoint risks, IT teams can ensure endpoint compliance, mitigate risks, and reduce exposure. FortiEDR provides additional protection by detecting and defusing potential threats in real time and can automate response and remediation with customisable playbooks.

FortiSandbox Cloud Prevents Advanced Threats and Automates Threat-Intelligence Sharing
When security solutions aren't designed to work together, the burden of creating automation and scaling to address the endless number of alerts from disjointed products falls on the business. The Fortinet Security Fabric answers this challenge with FortiSandbox Cloud. As a licencing option for the above solutions, FortiSandbox Cloud creates a central point for products to send unknown files. Advanced analysis determines their threat level and communicates this information across the Fabric. Threat intelligence is gathered from Fortinet customers around the world and shared, ensuring no matter where a threat was first encountered, the entire community has actionable intelligence.

Put Ransomware in its Place

As a Fortinet Gold partner, our experienced team can provide you with the expert knowledge to design and deliver the optimal security solution to protect against ransomware. Get in touch with us on 01280 878597 or email us at sales@optec.co.uk.