Whitepaper

mimecast

10 Ways to Prevent Ransomware Attacks

Ransomware attacks have been a reality for organizations of all sizes for quite some time. In recent months, however, the volume and sophistication of attacks, as well as the consequences, have been ratcheting up.

Companies that fall victim find themselves in an impossible situation. No one wants to pay—preventing ransomware altogether is the goal—but many feel they have no choice. Even worse, there are no guarantees. In recent research from Mimecast, 61% of respondents to an annual State of Email Security 2021 survey said they had experienced a ransomware attack in the last 12 months. Of those respondents, 52% paid the ransomware, but over a third never recovered their data.

So how do you keep your organization secure? It's about more than just security. Let's take a look at ten strategies that can reduce risk, build resilience, and help get attackers out of the driver's seat.

01.

Harden your email perimeter

As IT and security teams know all too well, email is still the top attack vector. The best way to prevent employees from falling for attacks is to block as many malicious emails as possible as close to the source as possible. Using a mature, cloud-based secure email gateway with advanced inbound and outbound scanning remains the most effective way to do that. For Microsoft 365 users, a layered email security approach is also essential to reducing risk, as attackers increasingly seek to reap the benefits of exploiting the world's most widely adopted business productivity platform.

02.

Archive to an independent, separately secured environment

The ability to protect and preserve corporate data can provide you with a greater degree of control in the worst-case scenario of a successful ransomware attack, while following the best practice of maintaining a lean amount of data can reduce your exposure and attack surface.

Archiving to an independently secured environment allows you to achieve both of those objectives.

03.

Build resilience with integrated recovery capabilities

The ability to quickly and easily restore mailboxes to a point in time can keep your organization functioning and mitigate the damage of a ransomware attack. It can also prevent your IT and security teams from devoting weeks or months to recovery efforts. This capability is particularly critical for M365 users, who often discover too late the data recovery gaps in the platform.

04.

Establish an email continuity plan

Disruption of mail flow is a reality that all organizations must face and plan for, and it can occur for a variety of reasons. Ransomware is definitely one. The need to apply urgent patches, remediate an incident, or even rebuild entirely using a clean infrastructure are others. Because email is still the lifeblood of the vast majority of businesses, the ability to keep it functional during disruptive events is foundational to a cyber resilience strategy. A continuity solution can ensure that when email goes offline, your business doesn't go down with it.

05.

Limit attackers' ability to craft highly targeted attacks

Highly targeted attacks that imitate a brand or use personal information are difficult for even the most sophisticated users to detect; and when it comes to lucrative targets, attackers are willing to put in the time to craft them.

Newer tactics, like the use of embedded email trackers, can reveal a target's physical location, operating system, level of engagement with the malicious email, and more. Combine that information with the ability to send spoofed emails from trusted email domains or easily imitate a digital presence and you have a serious threat on your hands. Protocols and technologies, such as DMARC and identity graphing, that complement email security capabilities can shield users from these targeted attacks and provide added layers of protection for you, your customers, and your partners. Learn more.

06.

Employ new technologies to improve the detection of sophisticated attacks

AI, and especially machine learning, are playing a growing role in cybersecurity technologies and can be a highly effective means of bolstering the capabilities of the solutions that leverage them.

The most common application to date is the recognition of patterns and the ability to build on that "knowledge" over time, allowing detection rates to improve. There's no question the use cases will grow, but it's also essential to recognize AI for what it is—a complement to a strong cyber resilience strategy, rather than a silver bullet. Technologies that incorporate it in an integrated way, with a long-term plan for how AI usage will evolve, can make your security strategy more effective today and help it stand the test of time over the long haul.

07.

Surround end users with support

When threats break through, security teams have no choice but to rely on the most unpredictable form of protection of all—human beings. There's little debate that giving them the knowledge and tools to make better decisions should be a key part of any organization's security strategy. The benefits of a cybersecurity awareness training program are many, but they are most effectively deployed as part of an overall strategy. Solutions that incorporate detailed tracking and risk scoring capabilities can help security teams identify the most at-risk employees, while reporting from email security systems can also surface those who are being targeted most frequently. Factors like these can then be used to provide additional support where needed.

In addition, tools like customizable warning banners and alerts—when applied in a selective and dynamic way—can go a long way toward helping employees make better decisions. Input from employees can also feed into your larger threat picture to further improve detection rates. Learn more.

08.

Maintain good patching hygiene

It goes without saying—but still bears repeating—that good patching hygiene is essential to reducing the risk of all types of cyberattacks.

Maintaining an inventory of your assets, monitoring for patches, and establishing clear prioritization processes are all foundational steps. Having a separately secured backup of data is also an important safeguard.

09.

Protect against drive-by download infections

Malicious files downloads can open the door to ransomware attacks that are difficult to detect. Technology known as browser isolation can reduce this risk by executing files remotely—in a container or in the cloud—to keep malware infections away from users' computers, devices, and networks. It can also help eliminate the patient zero problem.

10.

Monitor and control shadow IT

The new digital workplace has blurred the lines between professional and personal and reduced the ability of IT and security teams to maintain control. Insecure websites, poorly secured Wi-Fi, and unsecured file sharing services all increase risk. Application visibility and control capabilities can help. Designed to help IT and security teams address the "shadow IT" problem, they surface which apps are being used, by whom, and how often. Teams can then block or monitor usage as needed.

In addition to these ten key steps, no discussion about ransomware would be complete without a mention of cyber insurance. The debate continues to rage, with government officials starting to weigh in, and there is no clear answer. Organizations must each make their own risk-based decisions; but insured or not, the best strategy is one that makes the risk of needing to pay a ransom as low as possible.

Mimecast's mission is to stop bad things from happening to good organizations.

For more information on how we can help defend against ransomware and other sophisticated attacks, request a custom demo or visit Mimecast.com.