Digital Security
Progress. Protected.

Ransomware: How to provide a valuable layer of protection to email

As we discussed in our blog exploring Remote Desktop Protocol, ransomware is on the rise, and has been exacerbated by the current work-from-home trend. While the bad guys use many attack vectors to attempt to infiltrate your systems and plant ransomware, the most popular – by far – remains email.

Criminals either use compromised links or infected email attachments to deliver downloaders that install malware on the recipient's machine, or to establish a foothold on the corporate network.

This initial stage of a compromise can remain undetected for years before maturing into a full-blown ransomware attack. At this stage, it will look to steal valuable data and encrypt files, prior to making a ransom demand that can run into the millions of dollars.

It is important that everyone in your organization understands ransomware. Encourage staff to report suspicious messages and attachments as soon as they see them. Early warnings can help the organization fine-tune its spam and content filters and bolster its defenses.

Don't become an easy target

Cybercriminals are cunning. They are constantly coming up with new and innovative ways to fool corporate networks and the staff who use them. It's not just junior staff who are targeted using social engineering tactics, though.

In 2017, a managing director at a four-star hotel in Austria's Alps got a ransomware email that was disguised as a bill from Telekom Austria. After clicking on a link within the email, the hotel's electronic doors became unusable, and staff were unable to issue new card keys to guests. Those behind the attack demanded a ransom be paid. However, there was a further sting in the tail. After dutifully paying the ransom, the hotel was hacked three more times. This proves that by paying the ransom, organizations can also make themselves easy targets in the future.

Paying ransom is never a good idea. There is no guarantee the company´s data will be restored. As in the example above, once attackers mark your company as an easy target, it is very difficult to dig yourself out of that hole.

Remember, **prevention is always better than dealing with the consequences**.

Playing in the sandbox

Remember the threat landscape is not static. Cybercriminals are always looking to remain one step ahead. Businesses can mitigate the risk of so-called "zero-day" threats being used to implant ransomware by using a sandbox. A **sandbox provides a powerful, isolated test environment in which a suspicious program can be executed** and its behavior observed, analyzed and reported before it has the chance to do damage.

The right security solution can automatically decide whether a suspicious or unknown email attachment is benign or malicious by sending it to a cloud-based sandbox for analysis. By doing so in the cloud, there is the added advantage of offloading the processing power needed to detect unknown threats from employee machines so as not to impact their productivity.

Quick. Intelligent. Dynamic.

Email may not be the only attack vector, but it certainly continues to be popular for ransomware attacks. Ensure that you do all you can to provide a valuable additional layer of protection. Remain vigilant and analyze suspicious or unknown email attachments with a sandbox based upon the latest machine learning technology. It's quick. Its intelligent. It's dynamic. Above all, it's effective.