



CxO Fraud, Phishing, Ransomware: Powerful Security with Advanced Threat Protection

The challenge

A major part of electronic mail nowadays consists of unwanted messages. Along with the flood of usual spam and virus mails, companies and employees now also increasingly find themselves facing complex threats, such as social engineering and phishing attacks. Traditional security mechanisms often no longer provide sufficient protection from these personalized emails. Malware is now, moreover, altered at ever shorter intervals and constantly circulates in new variants.

The background

When they first appear, new threats are by nature unknown to virus scanners. As no matching signatures are as yet available, infected emails spread within a very short time. Adding to this dynamic, cyber criminals are employing increasingly sophisticated means of attack, with which fraudsters try to get hold of sensitive information. Conventional security solutions find it difficult to differentiate between such emails and legitimate messages. Successful attacks not only lead to data losses with serious consequences or the failure of systems, but also enormous costs and reputational damage. That's why it is crucial that companies adapt their security policies to meet current realities.

The solution

The Essential Protection provided by Retarus E-Mail Security already makes use of comprehensive safeguarding measures and up to four different virus scanners, enabling it to reliably filter out the vast majority of dangerous emails. With the enhanced protection offered by Advanced Threat Protection, companies can now employ a wide range of additional functions to secure themselves against those threats that go beyond the classic virus and spam emails.

Customer benefits

- ✓ Safeguards sensitive business communication
- ✓ Future-proof IT security
- ✓ Avoids financial losses through fraud
- ✓ Educates staff about phishing, etc.
- ✓ Provides protection from reputational damage due to loss of data

Benefits at a glance

-  Reliable identification of new variants of malware and virus
-  Enhanced protection against social engineering
-  Analysis by means of highly specialized data sources and own algorithms
-  Detailed reports and analyses
-  Seamless integration with other email services provided by the Retarus platform

Use Case

Criminals are increasingly using social engineering to launch attacks which entail the risk of financial damage to companies. In CxO fraud scams, for instance, cyber criminals pose as the managing director of a company and use bogus emails to instruct their victims to transfer large sums of money. Retarus CxO Fraud Detection makes it possible to recognize the fake sender addresses used for these targeted attacks and alert staff about fraudulent emails. This is achieved by means of an advanced analysis of the email header and specialized algorithms, which reliably identify from-spoofing or domain-spoofing.

In addition, Retarus Time-of-Click Protection also facilitates the prevention of phishing attacks and the resulting loss of sensitive data. The technology also checks all links contained in emails for target addresses which are suspected of phishing. If new intelligence gathered in the meanwhile shows that the target destination may be dangerous, the link is blocked and the user is instead shown a security warning.

To better protect companies from continuously developing and evolving malware, such as ransomware, Retarus also offers Deferred Delivery Scan as well as in-depth Sandboxing analyses as components of its Advanced Threat Protection. Deferred Delivery Scan involves a delayed re-scanning of selected attachments. To achieve this, the email is held back for a few minutes before it is delivered to the recipient. The delay means that for attacks using brand new malware updated virus signatures may already be available after a very short time which were not at hand when the first scan took place. With the Sandboxing solution also offered as part of Advanced Threat Protection, attachments are executed in a virtual, secure test environment and examined for irregular behavior by means of complex simulation procedures before they are delivered to recipients.



Did you know?

More than 390,000 new cases of malware are registered around the globe each and every day. This constitutes an average of around 270 new variants of virus per minute.

Other scenarios

Postdelivery Protection

Retarus' innovative Patient Zero Detection technology additionally identifies harmful emails which have already been delivered. Where suspicion is aroused, administrators are immediately informed so that any further damage can be prevented.

Secure Encryption

Sensitive data should never be allowed to fall into the wrong hands. With Retarus E-Mail Encryption, companies can ensure the confidentiality of their communication and comply with the applicable data privacy and protection regulations without difficulty.

E-Mail Live Search

With E-Mail Live Search, Retarus provides a service for quick and efficient analysis of email delivery. Your support employees at a company are able to track in detail which security filters have been applied for each specific message and when the email passed through which points in the infrastructure.