Image: TÜV Rheinland ©

FAQ – Cyber crime and Advanced Persistent Threats

Do you want to know more about Advanced Persistent Threats? We have compiled the most frequently asked questions for you below.

1. WHAT IS MEANT BY THE TERM "CYBER CRIME"?

A basic distinction is made between "opportunistic" cyber crime and organized cyber crime. The first involves attacks that are not aimed at any specific company with a goal of infecting as many victims as possible (e.g. ransomware, phishing mails, etc.). The second involves well-organized groups that are highly specialized and have immense financial resources with the goal of specifically attacking companies or critical infrastructures (in the form of complex, well-targeted attacks or APTs).

2. WHAT IS RANSOMWARE?

Ransomware is malicious software that allows an intruder to block access or use of data or the entire computer system. The victim is usually extorted with a "ransom".

3. WHAT IS AN ADVANCED PERSISTENT THREAT? (TARGETED ATTACK)

Advanced

An APT is a cyber attack launched against a specific company, person or institution. These attacks are usually deployed by well-trained attackers using advanced technology, strategic tactics and the necessary (financial) resources. Common cyber crime is aimed at no specific parties and attempts to maximize the number of victims, whereas APTs are well-structured and complex.

Persistent

After infection, the attacker attempts to go undetected for as long as possible in order to spread throughout the system and network. Usually, back doors for remote control

® TÜV, TUEV and TUV are registered trademarks. Their use and exploitation requires prior consent.

www.tuv.com/en/apt

TÜVRheinland®
Precisely Right.

are implemented, and information is collected, manipulated or diverted.

Threat
An APT is the most serious and damaging threat for a company.

4. WHO IS AFFECTED BY APTS?

According to Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.), medium-sized companies are most seriously affected by IT espionage or sabotage – over 60 percent. Most organizations are already compromised without even being aware of it. For the identification and well-targeted handling of security incidents, companies are often overwhelmed – both in terms of technology and the special expertise required.

5. HOW CAN CURRENT CYBER ATTACKS BE IDENTIFIED?

Innovative security technology and experts with mastery of these technologies are needed to identify and successfully defend against cyber attacks – both opportunistic and targeted attacks.
Conventional security systems such as anti-virus scanners and IDS systems are usually no longer able to identify sophisticated attacks used by cyber criminals to gain access to your company's data.

6. WHAT IS THREAT MANAGEMENT?

The term "threat management" refers to the totality of measures and solutions used by companies and organizations to manage their cyber security.

- Our APT Defense Service offers you a managed security service from a single source and as a service combining one of the leading breach detection solutions with incident response.
- Our Security Operation Center (SOC) can also expand the scope of managed service to include other of our security solutions.
- Our professional services also include a large selection of options (solution components from various manufacturers as well as consulting services) for effective threat management for the long-term improvement of your cybersecurity situation.

7. HOW CAN I GET AN OVERVIEW OF MY CURRENT SECURITY SITUATION?

- To start off, our Compromise Assessment Appliance monitors your network over a period of four weeks to determine the current status.
- After 14 days, you receive a progress report, and after the analysis phase is complete, we prepare a final report to provide you a detailed overview of the current security situation. Based on these findings, we determine which technical solution is appropriate for you and where it can be integrated.
- After implementation, our experts train your staff and set up the necessary processes together with you so that you can coordinate the proper response to attack incidents.

8. HOW DOES THE APT DEFENSE SERVICE WORK?

Technical requirements: The procurement of complex hardware is not required. TÜV Rheinland only integrates small, inexpensive sensors in monitoring mode (TAP) into the customer's infrastructure. These sensors perform a preliminary analysis of the company's network traffic (web, e-mail, etc.).
Detection of anomalies: If the sensors detect signs of an attack or infection, the suspicious network traffic is forwarded in fully encrypted form to a TÜV Rheinland data center.
Qualification of the security incident: In the TÜV Rheinland environment, the potential damage of the traffic is examined, e.g. tested to see how this data behaves when viewed or executed.
Limiting the attack: The experts from TÜV Rheinland use a managed security service to examine and assess the results. In case of an infection or attack, well-targeted defense measures are determined and the customer's internal IT staff is assisted in taking specific defense measures.

9. WHICH COMPANIES ARE GOOD CANDIDATES FOR THE APT DEFENSE SERVICE?

Innovative security technology and experts with mastery of these technologies are needed to identify and successfully defend against cyber attacks. This is usually only possible for large companies with their own cyber defense centers (CDC). The APT Defense Service now offers medium-sized companies an affordable managed security service for protection against cyber attacks.

10. WHEN DOES THE APT DEFENSE SERVICE BECOME ACTIVE?

Thanks to constant security monitoring, security incidents are identified immediately and automatically. The information is then provided in real-time to TÜV Rheinland CSIRT for analysis, evaluation and to plan corrective action. The APT Defense Service offers your company a highly innovative, behavior-based sensor technology to protect against cyber attacks.

11. HOW CAN THE APT DEFENSE SERVICE BENEFIT ME AS AN INFORMATION SECURITY OFFICER?

Planning reliability thanks to security-as-a-service: Once the sensors are installed, you do not have to take care of any operational tasks unless a security incident is identified.

12. HOW CAN I BENEFIT FROM APT DEFENSE SERVICE AS A COMPANY OWNER?

Protect yourself and your company assets against attacks and minimize potential damage and costs required to restore your good reputation. In cooperation with experts from TÜV Rheinland, your IT staff is able to work efficiently knowing they are well-protected.

YOU HAVE ANOTHER QUESTION? CONTACT ONE OF OUR EXPERTS NOW – WE ARE HAPPY TO HELP.

ONLINE CONTACT

® TÜV, TUEV and TUV are registered trademarks. Their use and exploitation requires prior consent.

TÜV Rheinland i-sec GmbH
Am Grauen Stein
D-51105 Köln
Tel: +49 221 806 – 0
service@i-sec.tuv.com
www.tuv.com/en/apt

TÜVRheinland®
Precisely Right.