Protection against Advanced Persistent Threats with Swisscom Managed Security Services (MSS-i)

Changes to the attacks

Over the past few years, Advanced Persistent Threats (APT) have been proven to be one of the most efficient cyber weapon. Advanced Persistent Threats are a combination of various methods that are used for targeted attacks on companies. The scope ranges from available exploits to the exploitation of vulnerabilities and even to specially developed malware. Here, mobile users' systems (laptops, smartphones, etc.) are particularly affected. Attacks are specifically aimed at these terminal devices as they repeatedly establish connections to the company network in order to use company resources (e-mails, file servers, etc.).

Consequently, today's attacks no longer take only a blanket approach, generating a huge amount of traffic, but take place quietly and are specifically targeted at companies and their systems. The aim is to steal information that can then, for example, be sold on for a profit. Infected systems usually transmit sensitive data to external systems over a longer period of time (months or years), remaining hidden in the company while doing so. This is why early detection – if possible real-time detection (Zero day) – of malicious data traffic by means of Advanced Threat Protection (ATP) is a key component of an effective solution.

Current installations usually consist of numerous security systems (firewalls, intrusion detection, AV scanners, proxies, etc.) in the form of appliances at the customer's site. These infrastructures are a key component and must be synchronised with one another as a chain. However, this alone is not sufficient to detect or block APT attacks. These classical systems detect attacks by known systems based on signatures (known patterns). Zero-day attacks, communication with suspicious networks and addresses (botnets, sinkholes, malicious hosts/URLs, phishing, etc.) and Internet services (e.g. TOR) cannot be detected using these means. To identify these, solutions are required that can make use of various mechanisms (e.g. log data analysis, filtering and detection, behaviour analysis, etc.) to detect attacks or infected systems and to raise the alarm, block or remove them.

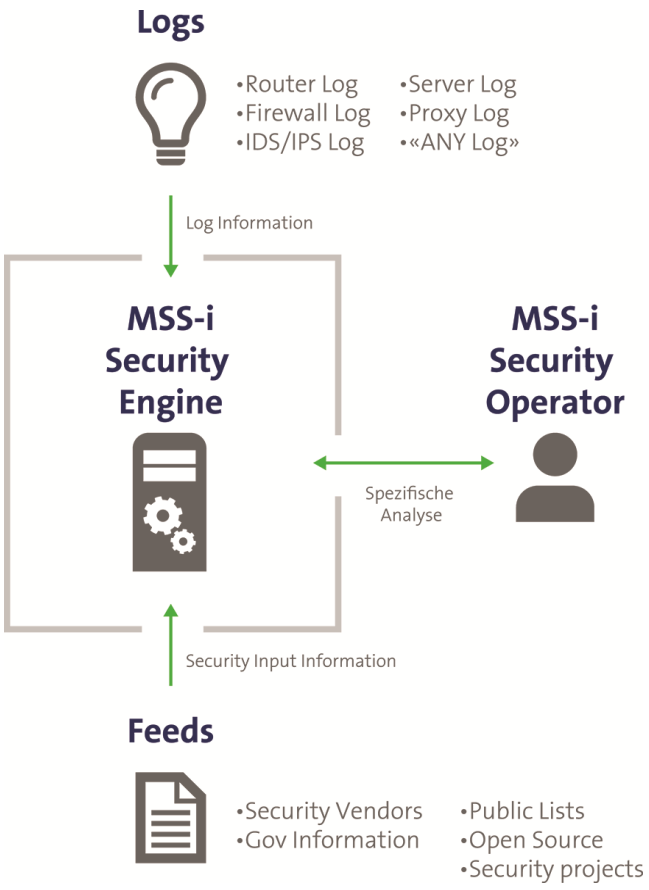
Multi-level protection against Advanced Persistant Threats

Swisscom operates security systems (firewall, IDS, VPN Gateway, proxy, etc.) by means of a managed security service. The systems are monitored around the clock and continuously run at the latest security level with new patches and releases, which is an elementary component of a protection system. Thanks to intelligent correlation – known as Threat Intelligence – logs and alerts from these systems are examined for threats and their potential security loopholes.

To recognise threats early and draw the right conclusions from them, Swisscom relies on many different factors. After all, the more precisely and quickly the Swisscom specialists find out where threats lie, the more target-oriented their can actions and reactions can be. For this reason, Swisscom continuously optimises and analyses its own and Swiss security feeds as well as feeds from international partner companies.

Key factors for efficient protection:

- Switzerland network: Nobody knows the Swiss network better than Swisscom. Information on the latest threats that are detected on the Swisscom network are immediately input into the service intelligence. Collective intelligence: Swisscom manages security devices in Switzerland and throughout the world. And, when analysing the logs, learns about concrete incidents around the globe. This ensures a "collective intelligence", from which all customers ultimately benefit.
- Smart correlation: Swisscom processes feeds and logs practically in real time: the logs are compared with the feeds and detect threats in a short time. The service compares the logs with the feeds in an intelligent manner. This correlation of big data ensures significantly more security than an evaluation using a simple algorithm. If a threat is detected, the system automatically triggers an incident.
- Expertise: Our highly trained security operators are available around the clock in the Swiss Security Operation Center (SOC), where they examine and evaluate the security incidents.



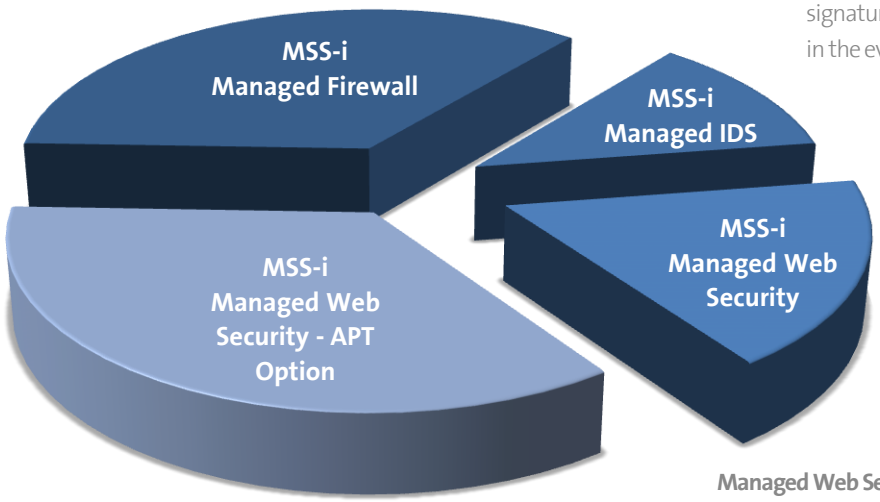
Modular services tailored to your needs

With Managed Security Services from Swisscom, you get a tailored protection against Advanced Persistant Threats. The modules are designed in such a way that they build on one another and can be added to.

Effective Threat Intelligence with modular Managed Security Services:

Managed Firewall
As the first line of protection against attacks, the firewall blocks or allows the data traffic on the basis of ports between the various networks.

Managed IDS
The Intrusion Detection System examines the data traffic for known weak points and attack patterns with the help of signatures and raises the alarm in the event of an incident.



Web Security – Option APT Protection
On the basis of the Managed Proxy Service , the APT Protection option can be activated, which scans and classifies every call up of a website. Furthermore, activities such as iFrames, cross-site scripting, phishing, cookie theft, zero-day exploits, malicious URLs, malicious hosts, XSS, viruses, adware, spyware, malicious JavaScript, malformed files, botnet C&C traffic and attacks on browsers and their third party plug ins are detected and blocked.

Managed Web Security
Web security protects your clients (desktop PCs, smartphones, tablets, etc.) and servers against dangers from the Internet (advanced threats). The connection (encrypted and unencrypted) from the end system terminates at the proxy and is protected against known dangers through the URL filter and anti-virus scanner.

Interested to further Information about our Network Security Services? Visit www.swisscom.ch/mss-i or contact us by sending an Email to ProductManagement.Security@swisscom.com