Central Threat Intelligence with Blue Shield Umbrella

IT Security of the Future

Central Threat Intelligence with Blue Shield Umbrella

IT Security of the Future

Current security situation

Nowadays, businesses of all sizes and sectors constantly face risks and threats from the internet. Regardless of whether it is a broad and random attack (e.g. ransomware), or a targeted onset (e.g. CEO Fraud), internet criminals most often strike undetected and smartly. The damages caused can be of tremendous and even an existence-threatening extent. On the radio, on TV or in the press – such cases are reported on a daily basis. Moreover, cyber-crime attacks become increasingly commercialised. The business model of the future lies in Malware-as-a-Service where control servers and malicious software are for hire.

How do businesses perform cyber security?

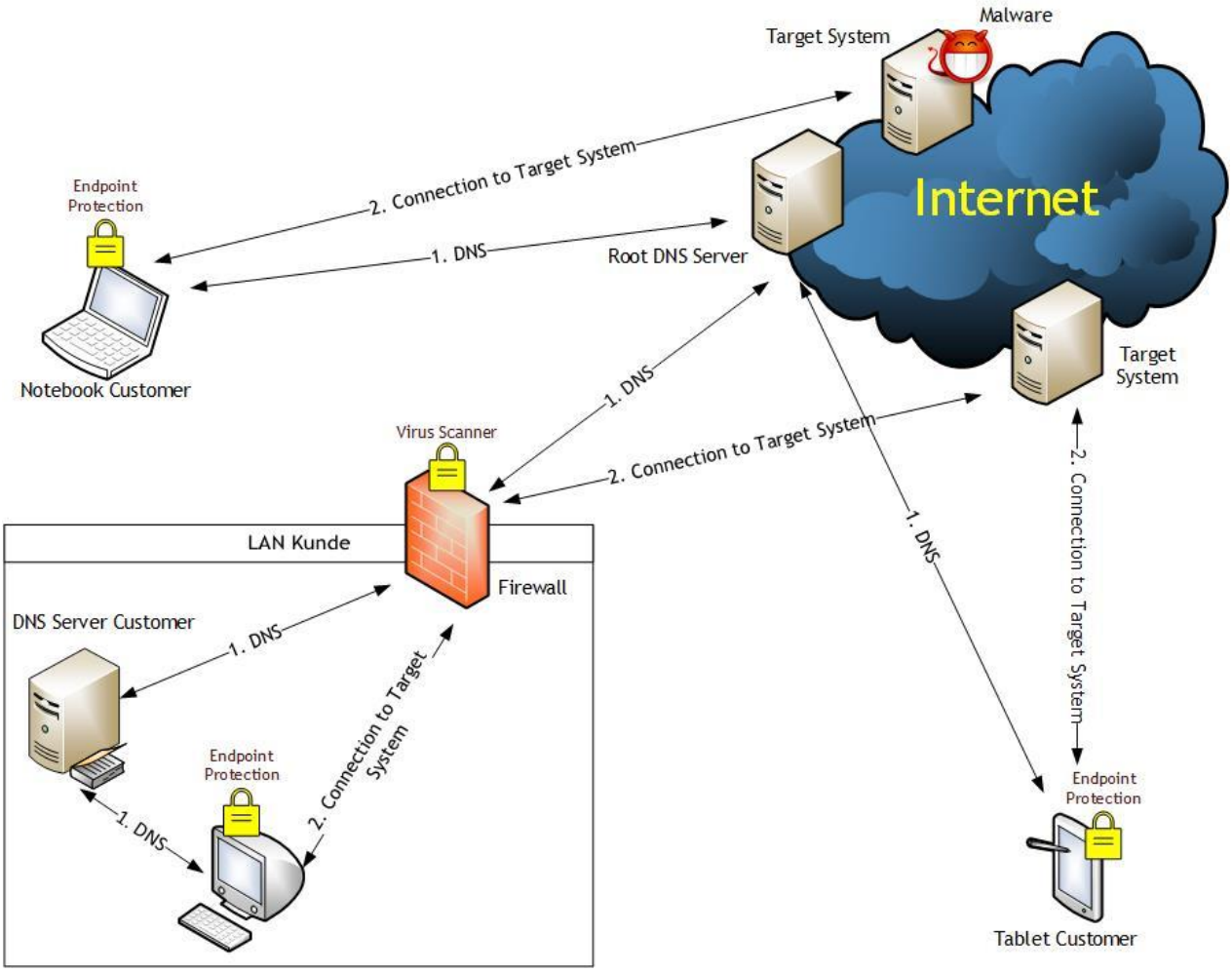
Beside projects and the usual day-to-day operations, IT departments of businesses are increasingly concerned with dangers that come from cyber space. Protection for companies is often rolled out in multiple components; this includes firewalls, sandbox systems, intrusion prevention systems, endpoint protection and so forth. Everything is geared to protect data and infrastructures from getting compromised.

Ideally, the interception of malicious software happens at or even before the network transfer point to the LAN by using firewalls, Anti-SPAM, proxies and intrusion prevention systems, for instance. If harmful contents break through, then the endpoint protection intervenes and provides protection.

However, all those systems must continually be updated and monitored. The administrative effort needed is substantial when one expects a well-functioning security system. And despite all that, internet criminals succeed again and again with the newest malware that outsmart IT security systems.

BlueShield

Internet Communication Standard Today



Once the malware has penetrated the LAN, it is often too late for counter-measures to be effective.

How current virus scanners work

Virus scanners work with different methods to spot malware. The most important and utilised ones shall be elaborated in brief as follows:

Signatures
To identify and isolate known viruses, anti-virus producers distribute so-called signatures to their clients. This method however is only effective, if the malicious software has already been detected and is known. In addition, the generation and distribution of a signature is very time-consuming.

Heuristic
That is the term describing the search for generic features and salience to detect still unidentified malware. This requires extraordinary intelligence of the anti-virus software, as 'normal' programmes shall not be affected, which involves great effort to programme and to keep up-to-date.

Sandboxing
Under this method, the alleged malware is incited to get active in a virtual environment. As soon as the malicious software starts to act, it can be identified and isolated without getting into the live system.

Behavioural Analysis
Similar to the heuristic and the sandboxing, behaviour is analysed here as well; however, this happens with the aid of algorithms (e.g. genetic or trainable ones), as well as statistics and neuronal networks. It is a very effective method; however, it normally can only be performed within the live system in real-time.

The problem lies in the nature of things

Most IT security solutions work with the methods as described above, which do not adequately correspond with the state-of-the-art any longer. The producers of malicious software test their programmes with the latest virus scanners in order to determine the recognition rate. Most malware is able to recognise sandboxing and so does not react until released from the virtual environment. Hostile software becomes more sophisticated and complex, it can easily and automatically be modified, so that pattern detection becomes rather ineffective. As a result, reaction to new threats is staggered. Once the malware has penetrated the LAN, it is often too late for counter-measures to be effective. Modern malware is also capable of keeping itself updated by downloading latest software components. Furthermore, current endpoint protection systems present challenges to the performance ability of workstation systems. In short: The IT security sector lacks substantial innovation.

The solution Blue Shield for full protection against malware is Umbrella

Harmless appearing emails, compromised websites and so-called drive-by attacks are the most common ways to transfer malware to the target. From there, almost 100% of malicious software are capable of loading a malicious code via the internet that enables them to launch and carry out the attack within the LAN.

This happens almost exclusively by means of DNS (name resolution). The link within an email leads to a compromised server via a name, there it downloads a malicious code and executes it immediately or time-controlled without being noticed by the user. The problem is that via name resolution, the link is not instantly recognised as compromised and so the attack can take place in the meantime. Depending on the quality of the security systems in place the attack cannot be prevented most of the times, but at least it can be discovered and at best, halted.

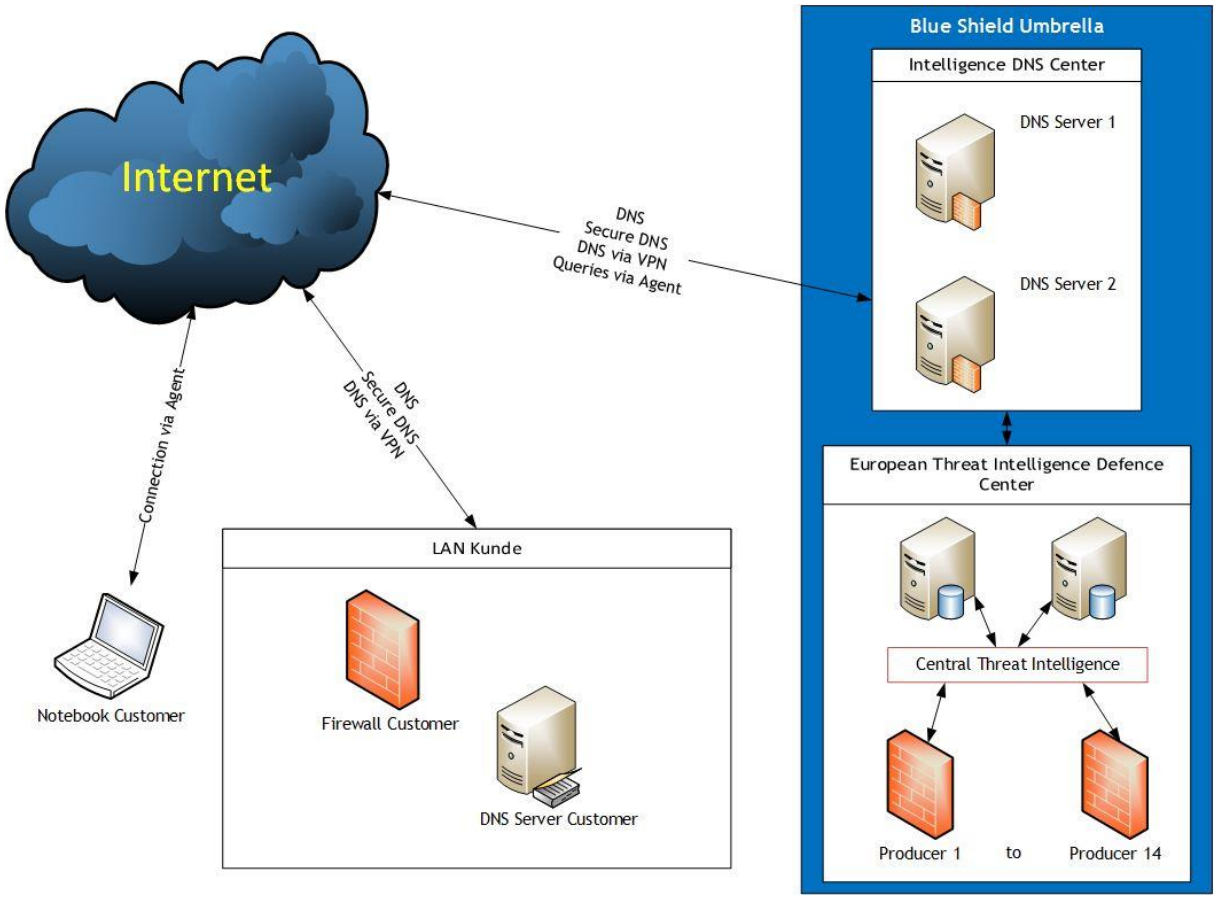
In order to prevent the attack, the name of the compromised system must be known and then blocked. This provides the full protection so that malware cannot infiltrate IT systems. The name servers in the LAN, a DNS proxy, a firewall or a router resolve your name request locally and redirect those in case of need to a so-called root-DNS-server. There, they receive answers to the name resolution and forward these to their clients.

With Blue Shield Umbrella the Intelligence DNS Centers are requested for name resolution instead of the root-DNS-server. Those further communicate with the European Threat Intelligence Defence Center and receive an assessment about the inquired names in real-time from there. When a name is blocked, the inquiring server will be informed about it and the clients receive a notification about the blocking. Through this innovative technology, an attack is halted before it even takes place and the download of malicious codes is prevented. In addition, the activities of existing botnets, Trojans or similar is shorted with this modern technology. Communication with the control servers is no longer possible and the malware becomes inefficacious. Hostile software cannot communicate with the control server any longer but communication is still sought and attempted; as a result, the computer contaminants become apparent in the LAN.

The European Threat Intelligence Defence Center reviews with numerous techniques the inquired servers in the internet for compromise and saves the results in a database. In addition, mathematical computations are in use. Therefore, the risks and threats are not only recognised but also barred.

BlueShield

DNS Communication with Blue Shield Umbrella



- Central cloud based Threat Intelligence
- Fast and flexible due to DNS use
- Protects all IP based devices
- Windows/MacOS/IOS/Android/Linux/ Internet of Things/Industry 4.0
- Easy deployment by means of Software-as-a-Service

Implementation, simple as that

Most IT security solutions require huge efforts for the implementation in the LAN and before becoming operational, as well as training staff of IT departments; nothing of all this is necessary with Blue Shield Umbrella. Solely the changeover to the Intelligence DNS Centers has to be done. This involves the configuration of the firewall in place so that it only permits inquiries for the name resolution from authorised DSN servers in the LAN. With regards to mobile workstations, an agent has to be rolled out, which ensures that outside the secure LAN the appropriate DNS server is being requested at all times and that this setting cannot be modified. Therewith the implementation is completed and the protection activated. It is as simple as that.

Blue Shield Umbrella does not make use of any resources (e.g. from hard drive, CPU, internal memory) in your system environment, because there is no installation of any software components. An installation is solely needed for the devices that are used outside the LAN.

Reporting and status reports

During the active protection you receive status reports, which give account of the averted risks and threats. Those can be viewed at any time in your personal clients' portal. That way you further can identify malicious software that is still existent in the system – at that point communication is blocked by Blue Shield Umbrella – to securely de-install and remove those once and for all. In addition, you are able to draw conclusions about the clients' behaviour regarding IT security and its utilisation.

The technical concept

On customer's side, an agent will be rolled out optionally for Windows notebooks and tablets, which ensures that outside the secure LAN the DNS server of the Intelligence DNS Centers are being used and that only those keep up and answer DNS communication. In the client's LAN, the root-DNS server at the DNS server will be deactivated and the Intelligence DNS Center's DNS server registered. At the LAN side of the firewall, a rule will be configured, which allows outgoing queries only via the authorised DNS servers in the LAN. The firewall obtains the DNS Server of the Intelligence DNS Center as the DNS server entry as well. The communication between the client and the Intelligence DNS Center takes place via agent, DNS, secure DNS or by means of a VPN tunnel. No sensitive or personal data leave the LAN during communication.

There are multiple Intelligence DNS Center that answer the clients' DNS queries. In addition, it assures communication with the European Threat Intelligence Defence Center. The Intelligence DNS Center is designed redundantly.

The European Threat Intelligence Defence Center is the core part of the system; it as well is redundant and analyses internet mail server and websites in real-time around the clock. Special mathematical algorithms and predictive analyses are used by the Central Threat Intelligence to compute risks and to subsequently block dangerous servers. Additionally, IT security mechanisms are retrieved from a pool of the 14 biggest security producers worldwide, and are incorporated in the assessment. It currently

constitutes the perhaps most extensive and securest procedure for website and mail server assessment.

Hence, Blue Shield Umbrella consists of the two components Intelligence DNS Center and the European Threat Intelligence Defence Center.

Target groups of Blue Shield Umbrella

Blue Shield Umbrella is suitable for every size of enterprise, as well as every imaginable line of business. Regardless of whether it is commerce, production, distributor or other branches of industry – everyone benefits from this innovative technology. Due to the easy implementation it is possible to provide protection fast and sound.

Particularly interesting is Blue Shield Umbrella for carriers. Through a central rollout and the central control of your clients' gateways, their protection can be increased significantly. Besides, an additional advantage can be drawn from this; the protection can be sold as additional business with an internet connection.

Even private persons and households can protect themselves easily by means of the Blue Shield Umbrella technology. By simply changing the name resolution at the gateway, the protection at home is guaranteed immediately and viable for the non-professional.

The Advantages of Blue Shield Umbrella at a Glance:

- ✓ Most innovative and modern malware recognition in real-time
- ✓ Combination of familiar recognition methods and predictive computation through mathematical algorithms provides best protection against malware
- ✓ Inspection takes place outside your LAN; therefore, potential malicious software cannot get into your net
- ✓ Easy implementation and roll out
- ✓ No software installation in the LAN necessary
- ✓ No consumption of valuable resources such as processing power, internal memory or hard drive
- ✓ No update mechanisms necessary; therefore, no reviews of any update functions
- ✓ No administrative effort
- ✓ Averted risks and measured efficacy accessible at the client's portal
- ✓ Independent from the IT landscape and operating systems in the LAN
- ✓ Protection also given with older systems, e.g. Windows 95 or XP
- ✓ Protection of proprietary systems and industrial IT components
- ✓ Absolutely no transmission of personal data

Glossary

Intelligence DNS Center

The Intelligence DNS Center provides the servers for name resolution. The client must forward all DNS queries to these servers in order to use Blue Shield Umbrella. They provide the communication to the European Intelligence Threat Defence Center.

Central Threat Intelligence

Internet servers are constantly examined with mathematical algorithms and the probabilities for threats are calculated here. Furthermore, the information gathered from selected IT security producers are compiled and processed in this place. All insights and results are fed into the databases of the European Threat Intelligence Defence Center.

European Threat Intelligence Defence Center

The European Threat Intelligence Defence Center, together with the Central Threat Intelligence, builds the core part of the Blue Shield Umbrella solution. The database servers are located here, which receive the results of mathematical probabilities calculations and information of selected IT Security Producers from the Central Threat Intelligence. From here, information and data is forwarded to the Intelligence DNS Centers. The European Threat Intelligence Defence Center is active redundantly in several datacenters.

Blue Shield Umbrella

Blue Shield Umbrella is one of the most effective, most modern and most innovative security solutions against malware. The solution consists of the cloud components Intelligence DNS Center, European Threat Intelligence Defence Center and Central Threat Intelligence. The end consumer only has to forward the DNS communication to the Intelligence DNS Center in order to enjoy Blue Shield Umbrella protection.

For further information:

Blue Shield Security GmbH
+43 732 211 922
office@blue-shield.at
www.blue-shield.at

Kornstrasse 7a
4060 Leonding
Austria