REDSOCKS
malware threat defender

Malware Threat Defender

Security 3.0

Total security: Cyber security and physical security rolled into one.

For the vast majority of people, physical security is second nature. We lock front doors, we hide our valuables, we don't leave back doors on the "latch," we close and lock windows and we are immediately more vigilant around people we don't know and trust. It is bred into us at an early age.

Just like in the physical world, cyber criminals aren't interested in the equivalent of low-value items. They're after our crown jewels, such as customer data, account details and intellectual property. But they're also interested in taking over or disrupting vital processes.

Physical and data security depend on each other, but surprisingly a number of companies still treat them as separate systems. Cyber security depends greatly on physical security. Attackers who can gain physical access to a network can almost always take advantage of that access to further their efforts. Simply getting access to a physical terminal where a memory device can be plugged in is usually sufficient.

Any technical security solution that is connected to the network must be protected to ensure that it cannot be turned into a tool to be used in an attack or for collecting vital security information. Consider for instance manipulating camera footage and completely shutting down parts of the detection systems. This doesn't only apply to the business environment but also, on a smaller scale, to a private environment.

Features:

- Immediate insight & action
- Preserving your security & privacy
- No impact on stability & performance
- Turn-key solution

Benefits:

- Filter determines own choices which you rely on
- Compliant with coming legislation
- Can detect & report unknown threats
- Pure Dutch, no dependencies of non-Dutch companies

The Solution

A holistic approach on the basis of security management. In view of the rapid development of cybercrime, a single and a physically and digitally integrated governance body for security becomes even more vital.

Addressing integrated security disciplines to ensure a cohesive security environment within an organization requires a number of coordinated actions to take place efficiently. Such actions include information sharing, collaborative planning, joint incident registration, new education platforms, shared risk management practices and much more. In short: An organization in which IT and physical security experts combine measures as well as resources to achieve pivotal security goals.

How does it work?

The MTD will be located next to the router sending your data to the Internet. The router provides the MTD with metadata about the network traffic. Metadata don't regard the content of the communication itself but rather its nature such as the originating and destination address, the protocol, the used port and the size of the communication.

The MTD therefore never looks at your confidential data; it only analyzes the characteristics of your data traffic.

RedSocks uses the "Intelligence Driven E-gress Security Model". Against a list of internet addresses of which we know that these addresses communicate with malware, the MTD continuously analyzes the metadata using this model. The algorithms and lists used by and made available to the MTD, are compiled and kept up-to-date on the basis of millions of pieces of malware the RedSocks Malware Intelligence Team analyzes every hour.

How will the world of physical security benefit from this?

The MTD enables you to indicate which communication you trust and which you don't. Communication with an address you don't trust will be reported by the MTD. It provides you with the option to take action, depending on the threat level established.

When you notice your address is used for communication with an address you don't trust, the MTD provides you with the option to perform a historic analysis over the last 12 months to see whether such communication has taken place before. It will again enable you to take action.

The continuity of your IT facilities is essential for your institution or practice. Don't take any risk and prevent malware from doing any harm.

WHY REDSOCKS?

RedSocks is a Dutch company that specializes in malware detection. RedSocks provides the RedSocks Malware Threat Defender as a network appliance. This innovative appliance analyzes digital traffic flows in real-time based on lists of malicious indicators and algorithms compiled by the RedSocks Malware Intelligence Team. The team consists of specialists whose job it is to identify new threats on the Internet and translate them into state-of-the-art malware detection.

VOOR MEER INFORMATIE KUNT U CONTACT OPNEMEN MET ONS VIA INFO@REDSOCKS.NL OF BEZOEK ONZE WEBSITE: WWW.REDSOCKS.NL

REDSOCKS
malicious threat detection

www.redsocks.

• Tel e)56)eeeeee E-mail info@redsocks.nl Website www.redsocks.nl