EVOX

INFO SEC

Secure Operations Centre.
Can you survive without one ?

27, Evagorou Ave. Irene Building Suite 54 Nicosia 1066, Cyprus
T: +35722022624 W: evoxco.com E: dlambrou@evoxco.com

EVOX
COMPUTING

EVOX COMPUTING

Are you ready to protect your Infrastructure?

Large organizations are heavily depended on their technology infrastructure to deliver business services either to internal users or to external customers. All your business services exist based on the assumption that your underlying technology maintains its integrity at all times. The complexity of today's IT ecosystems pose a significant risk on the integrity and confidentiality on your data.

Deploying perimeter security devices and endpoint protection systems are inadequate to protect data leakage and advanced attacks. However, It is absolutely necessary to deploy standard security technology, which will most of the times, protect you from an external or internal attacker with low commitment on compromising your systems or from an inadequately funded attacker.

It has been proven over the last couple of years that it is highly inevitable to keep your internal environment clean of "infections". Targeted attacks have a relatively high rate of success. It is not in the scope of this paper to cover advanced attacks, so we will only refer to the classic attack vectors.

INCIDENT RESPONSE

Do you remember the last time you had a security incident at your organization? If yes, then you should be able to answer the following simple questions

- How fast did you detect that a compromise is underway?
- Can you identify the exact time the attack instantiated?
- Did you quantify the systems the attack had already compromised?
- How soon where you able to contain the assumed risk?
- Are you sure all compromised systems have been checked?
- Do you have a clear audit trail of the attack incident?
- How would you rate your organization's overall response time and efficiency?
- Are you confident that all security incidents are detected?

COMMON ISSUES WITH STANDARD TECHNOLOGIES

There are three main issues with the standard approach for protecting your infrastructure.

1. Security devices and software can only detect malicious events

2. Security devices produce a high rate of false negatives alerts

3. Inadequate logging capabilities do not allow you to reconstruct a complex or even a simple attack incident.

Some of today's attacks are highly sophisticated and targeted. They will not exploit the common attack vectors being monitored. What would otherwise seem like legitimate traffic might actually be a low profile attack.

PREVENTION IS THE LAST STEP

In order to be able to prevent a possible attack you must be able to detect it first. For effective detection of a slow attack it is necessary to correlate between different technologies and have dedicated personnel to the task. So even if you do possess the necessary technology not having well trained and dedicated stuff and clearly defined policies and procedures in place to cover incident response will most likely prevent you from having a good sense of security in your organization.

Making it happen

A Secure Operations Centre is dedicated to detect, investigate and prevent any type of attack within your organization. What exactly does a SOC takes to build?

- **Facilities:** Computer equipment, special secure areas, HVAC
- **SOC personnel:** Security analysts, shifts and SOC managers
- **Education and training:** security training, conferences, hacking skills
- **Support:** Network support, systems team, database, security device management
- **Threat intelligence:** Up to date information on latest threats
- **Monitoring technology:** Hardware, software and storage
- **SOC Platform:** Change management, ticketing system, case management
- **Analysis platform:** Security lab for malicious software analysis, on demand analysis software

PEOPLE

Once you have clearly defined the SOC mission it is necessary to employ the necessary people for carrying out this mission.

Some operations require less skillful workers than others. You must be capable of identifying which operations are more critical and provide the most value in order to invest more on skills.

PROCESSES AND PROCEDURES

Processes and procedures are critical to the performance and to the realization of the SOC mission. The effectiveness of your SOC is heavily depended on how well written and complete your procedures are. It is not enough to write them once but instead you must always update them and enhance them.

SOC processes are broken up in four main categories:

- **Business processes:** Administrative and management components for effective SOC operation
- **Technology processes:** System administration, configuration and design
- **Operational processes:** Daily operations, shift schedules, activity reporting
- **Analytical processes:** Document all activities designed to detect and understand events

TECHNOLOGY

Another crucial factor for a successful SOC is the underlying technology and mechanism or tools. Your SOC must have all the necessary technologies for accomplishing its task. Remember you have terabytes of information to analyze and looking for an attack pattern might be difficult.

The most important are:

- On demand lab provisioning
- Visualization software
- Data correlation and statistical analysis
- Correlation engine with net modeling

SUMMARY

It is evident that operating a SOC is not an easy task and definitely not a cheap one either. There is a significant investment in building it and also maintain it. Keep in mind that it is not easy to prove the effectiveness and ROI of such an investment. Depending on the size of the organization outsourcing might be a choice. Outsourcing off course comes with its own pitfalls!

Evox Computing Services

Our value added services will help you make the right choice. We have highly skilled resources and vast experience in incident handling in real world scenarios. We know what it takes to plan a successful attack and we also know what it takes to detect it and quantify the associated risks.