From Acting to Reacting IT Security

Abstract

IT Security has been developed in the last years with a practical approach to defend our IT systems, from a purely Operational point of view to Monitoring and update the defences. But the trend of attacks and the software complexity with associated number of vulnerabilities, makes it quite likely that breaches will occur. Keeping with a practical approach to IT Security, it is probably most efficient to shift today the focus from an active to a reacting point of view, implementing strong Incident Response plans and managing Monitoring and Operational Security so to minimize incidents, breaches and losses.

In the last 20 years our approach to IT Security has improved greatly but this is not an indication of having reached our final goal: we still need to improve and to develop new approaches and processes for it.

The only possible starting way was to develop some tools to implement the first features of IT Security. So in the '90s we saw the first packet filters (or firewalls), the first access control procedures and so on.

To say the truth, IT Security existed already before that, but it was an area mostly approached with military security in mind, see for example the Orange Books [1] (or TCSEC) later evolved in the Common Criteria [2].

But the current IT Security started as the practical deployment of tools, configurations and procedures to design and protect the perimeter of each company's IT and filter the incoming, rarely outgoing, traffic. Again the practical approach brought to the introduction of Anti-Viruses and its industry. In general we now have what can be called “Operational IT Security”, a branch of IT which encompasses all practical measures to prevent Security Incidents.

Proactive IT Security

At that time we thought that with enough good proactive practical IT security we could make our IT systems "secure". Seldom an idea has proven so wrong. Obviously we have always known that perfect security is impossible, and that the perfect protection of IT information is possible only if no information is there so that there is nothing to protect.

But in practice we do not really need perfect protection, just enough protection against our adversaries. This seemed to be an accessible task.

But we did not consider correctly at least the following three issues:

- the complexity of software increases at a non-imaginable speed and at the same time the number of security vulnerabilities grows exponentially leaving too large an attack surface;
- the amount of communication, data transmitted and shared, people interconnected was not imaginable just 10 years ago;
- the human difficulty to use the IT tools and understand the risks associated to it, makes it quite easy for an attacker to find a venue to trick a user to let the attacker enter an IT system.

This means that Operational Security, the practical approach to defend our IT systems, cannot protect our IT systems even against not too skilled attackers.

Obviously, we must have Operational Security otherwise it would be like leaving the front door of a Bank open for everybody to enter and get what she/he wants, but we need something else to, in practice, manage IT Security.

The next step is to monitor the IT systems, networks and applications, to detect attacks and intrusions. The information produced by the monitoring of IT systems, networks and applications allows us to improve the operational measures in place, block attacks, remove malware and viruses that have been able to bypass the first security defences and so on.

Monitoring should be seen as a way of feeding the practical operation security with information on what and how to defend and protect the IT systems. This can still be part of the proactive IT security process, indeed the main purpose of monitoring is to detect an attack before it manages to pass all our defences and block it. It is a way of fine-tuning our proactive IT security based on what we have to defend against.

Reactive IT Security

But in some cases we do not manage to block all attacks in time for example because at that moment we do not have the right IT security measures at disposal, and the monitoring just tell us that an attack has been really successful. What should we do then? At this point, that is when we have detected a successful attack against our IT systems, we must intervene with what is usually called an Incident Response action. For this, we need to have in place an Incident Response plan and the tools and expertise, internal or from external providers, to manage and solve the incident.

This is a reactive approach to security, in that we act after the incident has happened and the damage has been done. What we do in this phase is to detect the damage, restore what can be restored and suggest new security measures to prevent it to happen again.

Obviously everybody hopes that this will happen very rarely, actually never. For this reason up to not too long ago, Incident Response plans were seldom taken very seriously, described in details or even practised and rehearsed.

The Three Areas or Approaches to IT Security

We have just divided the activities of IT Security in three areas: Operational Security, Monitoring and Incident Response. Just to be clear about what they mean, we briefly list activities belonging to each of these (without any attempt to completeness).

Operational Security

- IT and IT Security organization
- security of software development and hardware procurement
- physical security of IT systems
- technical IT security: external and internal network security, security of Operating Systems, application level security, user level security
- technical IT security: in particular managing of anti-viruses and similar applications, software updates & patching

- users' and IT personnels' procedural IT security
- security in IT project management
- risk based IT security covering all areas and at all levels.

Monitoring

- monitoring of network attacks
- monitoring of system attacks
- monitoring of application attacks
- monitoring of software vulnerabilities
- monitoring of 0-days disclosures and attacks
- monitoring of patch level of systems and applications
- reporting of monitored systems and of application of fixes.

Incident Response

- emergency patching
- 0-day defence
- new threats' analysis
- incident handling
- incident reporting and lessons learned.

From proactive to reactive IT Security

We can summarise our approach to IT security, as evolved in time, as follows. We started believing that it was possible to build a fortress around the IT systems and live “secure” at least for a long time. Then, not too long ago, we realised that our IT systems keep changing, the attacks keep changing, and that we need to constantly maintain the fortress. This implies that besides building the fortress we need to monitor it and keep updating it.

But now we are realising (for example see [3]), that even this constant monitoring and updating is not enough to keep our fortress impregnable. Actually we are sure that soon enough someone will be able to open a crack in our walls and enter our fortress. At this point we need to react and fight the bad guys out of it.

This implies that our attitude with respect to IT security must change. If it is possible or even quite probable that our defences will not hold the enemy at bay, then we must be ready to fight inside our own house. This is not a declaration of failure, but it is a different, typically more difficult, but unavoidable step we should take.

We are aware that IT systems are too complex to manage and to secure, and that they are getting every day more complex. We are aware that one of the major issue is the human-machine interaction, where "mistakes" made by the users are most of the time responsible for IT incidents. So it should not come as a surprise that our defences do not hold and we have security breaches some times with minor consequences, other times with major consequences. Knowing this, it follows that we should be prepared to deal with breaches, to discover them and fix them. That is, we need to put our efforts not only on the monitoring but also on managing the incident response.

Summing up, we still have to:

1. secure at best our IT systems by implementing all Operational Security measures
2. monitor the security of our IT systems
3. respond to any incident which will happen.

What changes is the focus and the efforts we should put in the three activities. Usually Operational Security takes all or the largest part of the focus and efforts, leaving a little to Monitoring and almost nothing, like an after-thought (since nothing will never happen, right?) to Incident Response.

This implies that our efforts are very unbalanced, we leave almost not covered Incident Response and just a little covered Monitoring.

But due to the high possibility of an IT security incident to happen, recently it is suggested by many to approach IT security from the opposite point of view:

1. build a strong Incident Response management, be ready for any kind of breaches and attacks;
2. this requires that Monitoring must work well to detect all attacks and breaches;

3. and finally, implementing the Lessons Learned activity of the Incident Response plan, we increase the IT Operational Security.

Of course, if you are building a new IT system you need to start from the basis, that is first implement a strong IT Operational Security, but then the current suggestion is to shift the focus to Incident Response and approach the management of IT Security kind of backwards, from breaches to fixes.

This is not very orthodox but actually it quite fits with the practical approach we mentioned at the beginning: try to make IT security work in practice, every day, at affordable costs and not too complex to implement. Even this goal is very hard to achieve, but any proposal or approach that can make it easier to reach, is welcomed.

References

[1] The Orange Book, DoDD 5200.28-STD, issued in 1983 and updated in 1985 by the National Computer Security Center (NCSC), an arm of the National Security Agency (NSA), http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

[2] “Common Criteria for Information Technology Security Evaluation” (abbreviated as “Common Criteria” or CC), ISO/IEC 15408, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341

[3] “A motivated, funded, skilled hacker will always get in, It's how you respond that's key (Schneier)”, http://www.theregister.co.uk/2014/10/09/your_security_defences_are_going_to_fall_get_over_it_schneier/

Andrea Pasquinucci (PhD CISA CISSP)