

Synopsis

This paper explores how a client's risk profile changes when using Intrusion Prevention Technology as opposed to Intrusion Detection Technology.

Risk analysis

Risk is defined as the likelihood of an event happening (probability) multiplied by the impact when the event takes place (exposure).

Risk mitigation actions can either affect the likelihood of an event-taking place or it can reduce the impact of the event or it can have an effect on both event likelihood and impact.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) are normally used to alert a company when intruders have entered their systems. This would trigger an incident response process that has many objectives, including the following:

- Manage the impact of the intrusion
- Reduce the likelihood of future intrusions
- Feed back into the operational and security aspects of the business to improve the business's security posture and limit exposure so as to reduce future risk

IDS plays a critical part in the Incident Response process, as it is responsible for triggering the process. It can therefore be said that, considering all Incident Response processes to be equal, the implementation of a good IDS can both reduce the **likelihood** of bad things happening to a company and indirectly the **impact** of those incidents.

The two critical assumptions mentioned in the previous paragraph are:

- All incident response process being equal and
- A good IDS implementation

What happens when that is not the case?

IDS itself is passive and cannot really do anything unless there are humans who can act on the information provided by the IDS. If the Incident Response group is very effective at fighting fires, then the exposure that the company faces will be reduced (the impact of each fire is now less). However, if they don't feed the lessons learned from each incident back into the company's security management and engineering processes, then the likelihood of future incidents is not really affected. This is also true of the converse if the Incident Response team is not very effective at fighting fires, but they are effective at changing the way the company does business to reduce future fires.

If a company employs inferior IDS, then the fight is over even before it is started as the Incident Response process is never even triggered.

It should be clear from the above analysis that a company's residual risk as mitigated by its IDS's is ultimately severely dependent on the performance of its Incident Response process.

In reality, very few companies have good Incident Response Systems and even if they spend a lot of money on IR, the nature of security failures are that these systems only get tested occasionally (one would hope!) and even then, it is difficult to continually justify the cost of maintaining such an expensive process when the more successful it is, the less it is needed.

Intrusion Prevention Systems

Intrusion Prevention Systems (IPS) differ significantly from IDS in that IPS actively terminates data streams that are identified as unauthorised.

If one assumes that IPS's are as effective at identifying intrusions as IDS's, then the IPS replaces a significant portion of the Incident Response process in a single heavy handed way, by terminating connections which it deems to be unauthorised.

If one again assumes a low occurrence of false positives (authorised data that is incorrectly identified as unauthorised) and one also assumes that the knee jerk reaction of immediately terminating an unauthorised connection is also the first action that your Incident Response team would have taken, then it looks as if IPS's are an automated way to manage risk and costs associated with your Incident Response process.

So, out of the box, the perfect IPS will **reduce your risk** by lowering the number of incidents (most bad connections are terminated on the perimeter) and it will **also reduce the impact** of incidents by increasing your company's security posture since the Incident Response team is now in the first place an automated response. The cost of Incident Response is now not only better known, but also vastly reduced because fewer incidents occur (If one defines an incident in this case as an attack that succeeds in circumventing the IPS).

But what additional risk do IPS's introduce to the equation?

- False positives will result in termination of authorised traffic (loss of service)
- The system is susceptible to potential DOS attacks by triggering the IPS on legitimate data.
- IPS can replace neither IDS nor the Incident Response process because it cannot catch all intrusions and by dropping the connection, you are managing neither your company's internal risk posture nor the likelihood that the external threat will not continue with other attacks.

Is it realistic to think that dropping connections is the correct first step in Incident Response? Opinions differ and again, I guess the answer lies in what your Incident Response Process looks like. If you have the capacity/energy/funds to monitor intrusions with the purpose of learning more about the intruder, then the dropping of connections is certainly not what you want to do. If you are, like most security teams in the real world, primarily concerned with the protection of your assets as a first step, then there is no better first step to take other than to terminate perceived intrusions. Nothing prevents you from tracking any other activity generated by intruders for further in-depth analysis.

False positives are an issue as an unacceptably high occurrence might severely impact on your business. However, considering the fact the your IPS will not drop a connection without alerting you to it (unless you tell it not to!) then the process is perfectly deterministic and through a process of analysis, you will identify and can reduce the frequency of false positives.

How to deal with DOS attacks? Most IPS's today can be configured to reduce the impact of DOS attacks. The reality is that with any type of DOS attack, there is no quick fix and your Incident Response process will have to deal with a large part of the management thereof, just like they have to for your regular network services.

IPS vs. IDS?

It should be clear from this paper that IDS and IPS play different roles in a company's security architecture and even though their internal working in some case might be very much the same, their management and operational functions differ completely.

IDS are primarily used to activate the Incident Response process and by itself can contribute little to the quantifiable improvement of your security risk. IDS are only as effective as the Incident Response team that monitors them.

IPS on the other hand is a little bit more rough handed with intruders and will kick off the first step of the Incident Response process by terminating bad connections. That in itself lightens the load on the Incident Response team and reduces your security risk in a quantifiable manner. The additional risk such as false positives and DOS attacks that IPS introduces to a company can be measured and managed in an acceptable way.

About CounterSnipe Technologies

CounterSnipe Technologies is dedicated to the provision of IT security products with a focus on maximum Active Protection of the corporate Infrastructures. The team at CounterSnipe have been working together since early 2002 to develop the flagship product - the Active Protection Device for in line protection of corporate assets. The emphasis is on ensuring a precision delivery of engineering elements in all of the products we build, ensures World class solutions for customers. CounterSnipe is a privately held company, headquartered in Atlanta, Georgia with an ever-increasing presence in the International market.

CounterSnipe Technologies
1230 Peachtree Tower
Suite 1800
Atlanta
Georgia 30309
USA