Technical Article

Infrastructure & Cities Sector
Building Technologies Division

Zug (Switzerland), August 28, 2012

Cyber threats – it doesn’t just happen in the cloud

There are very few organizations that are not in some way reliant on data. The protection of that data is fundamental to business, to governments and to security forces alike. Much is currently being made of the cyber threats posed by the cloud. The increased use of hosted cloud computing and virtualized environments has made the protection of the data centers that hold this information even more critical. But it is not just about ensuring protection from the cyber threats: the Trojan horses, viruses, malware, hacking and information warfare that characterizes the modern world; it is also about recognizing where those and other threats come from and employing physical security measures to complement the software based systems used to protect networks.

The security challenges faced today are many and varied. A security vulnerability is any flaw in an IT system that can be exploited by an attacker to compromise the confidentiality or integrity of a data set or system or to deny legitimate user access to the data or system. In terms of those posing the threats they can be external parties or people operating within an organization – or a combination of both. Intruders, criminals, spies, disgruntled employees, cleaning staff and contractors – these, along with many more, can threaten the security and reputation of a data center and, in turn, the security and business continuity of the customers that it serves. Likewise with large organizations that host the data themselves.

In preparing for attacks criminals are increasingly using social engineering and profiling to gain access to buildings. Tracking employees through social media provides a lot of information that can prove useful in posing as an employee to get into the building and the majority of data attacks typically include an inside role of some description – whether voluntary or not. Data theft, malicious uploading, data corruption and organized theft of intellectual property – all are issues which need to be addressed and there are countless examples worldwide on an increasingly regular basis. The wikileaks website demonstrates how widespread leaking of sensitive documents now is and also how quickly and easy it is to circulate these documents to the world. Classified documents concerning the Iraq war were downloaded by a soldier onto a USB stick and made public. In commerce, bank details have been accessed, including a case where employees of Swiss banks stole data and sold it to the German tax department. This is certainly cyber crime but it is not just about internal protection of the network systems.

One immediate and very real risk is the physical removal, destruction or manipulation of digital assets (data and applications), .e.g. through theft, sabotage and uncontrolled access to data or applications, all of which can be significantly reduced by combining network security measures with physical security, such as technology-aided access control protocols. Because the origin of a threat can be internal or external, and because security is about making it as hard as possible for a criminal to succeed. Enterprises and data center service providers alike need to consider implementing multiple layers of technologies that will deliver an “Outside-in and Inside-out “protection.

Protecting the perimeter

The first line of defence (or last line in the case of an insider threat) is perimeter security. Many blue chip companies are located in high profile buildings, often in the center of cities or close to them. This means that they do not want high chain link fences, gates and barriers around the perimeter: it is not attractive and in some cases it is not feasible because of planning restrictions in heavily urbanized areas. There is therefore a trend towards intelligent perimeter solutions, establishing virtual perimeters through the use of technology such as fibre optic cable or passive infra-red (PIR) motion sensors, along with surveillance cameras. Video surveillance is an area where there has been significant development. Video content analysis is now widely used to automate the alarm process rather than relying on security personnel simply to spot events. Trip wires can be set at specific points to raise an alarm if the perimeter is crossed. Automatic object detection can also be used to alert personnel to the presence of suspicious packages, vehicles, and persons, or behavior analysis algorithms can be employed to enable cameras to automatically detect suspicious behavior. With the increased threat of terrorist attack on high profile buildings, such algorithms make an important contribution. Significant research and development is also being focused on forensic analysis of video data, a point I will return to later.

Within the building

Moving into the building, video surveillance again often plays a role in monitoring and restricting access. Frost and Sullivan’s Analysis of the Global Vulnerability Research Market in Q3 2011 points to the rise of attacks on third party applications. Once an application has been weaken, any devices on the network can become a point of entry for further hacking. This means that protecting digital assets now also needs to include all peripherals as an extra measure – protecting critical areas (server rooms) is no longer sufficient, and combining digital and physical security measures needs to extend to the entire facility and asset pool. Integrating video surveillance cameras with an access control system can provide the means to verify the identity of a person entering an unmanned access control point by automatically capturing a video stream as their identity card is presented to a reader. This management of a person's ID is an important factor in maintaining the security of a building and its digital assets, with a number of verification options now available to ensure only authorized personnel have access to certain devices, applications or data sets. These include biometric technology, such as fingerprint or iris scanners, and PKI (Public Key Infrastructure) technology whereby two mathematically related cryptographic keys (one private and one public) are used to unequivocally prove the identity of an individual. In particularly sensitive areas, buddy systems may be employed, requiring two personnel to be present in order for access to be granted to download data, for example. If a pre-defined user role is violated, security personnel will be alerted to intervene. The nature of the building will dictate the appropriate level of security controls, striking the balance between the security required and the day to day operation of the facility.

Tagging hardware can also help to monitor access and reduce theft. For example, large data centers are increasingly tagging their racks so that any access, even if it is by an authorized engineer, is monitored. Revolving doors are widely used to provide exact tracking of the people entering a building, particularly useful in buildings where large numbers are working or visiting. By using integrated systems across multiple buildings on a given site, this can prove useful in mass notification systems. These are the systems designed to simultaneously warn people in an emergency situation, sending alerts and instructions through a range of media, including cell phones, computer screens, landline phones, closed circuit TV screens and public address systems. This highlights the move towards a more intelligent response to emergencies.

Intelligent Response through integration

Intelligent response relies on the data provided by the increasing integration of safety, security and other building management systems. Open architecture is very much a focus at the moment, with a move towards standardizing protocols to allow different systems, often from different manufacturers, to work together. This can include security, life safety - including notification systems - and comfort provided by heating, ventilation, cooling, lighting, and power management systems. Convergence is currently a widely used term in security. This is convergence in terms of the different systems working together but also between physical and IT security. Technological advances in video management, network cameras, recording devices, intelligent access control and software have helped security applications to take advantages of the IP network. Response systems of the future – Intelligent Response systems where the system in place involves a variety of fully integrated, multi-modal technologies – will take integration further still. With systems capable of analyzing all relevant data collected from the thousands of sensors and field devices and the various management systems operating throughout a building, a 'demand controlled' response to incidents will be possible. This data will automatically trigger the relevant system response mechanisms in relation to the nature, size and criticality of the incident, and enable the automated provision of dynamically updated and targeted instructions to everybody concerned, from guiding them quickly and efficiently to a place of safety to providing relevant situational information for swift and efficient intervention.

The benefits of such solutions are multifold: intervention is faster (supported by comprehensive situational information), mitigation is more targeted and efficient (the right systems are triggered automatically to e.g. extinguish a fire), and collateral risks are minimized (e.g. quicker return to secure building situation, e.g. access controlled doors locked etc). In addition, audit trail of actions taken and sequence of events can be leverage to facilitate the post-incident and recovery activities (insurance claims, liability risk management) and continuous improvements with regards to security and business continuity (policies and workflows).

Forensic analysis: video surveillance

Returning to the issue of forensic analysis, an area of significant development is the application of this approach to video surveillance systems. In the UK, a watershed event that was certainly a driver in developing this technology was the London bombings of 7 July, 2005 when 4 terrorist bombs – 3 on the London Underground network and 1 on a double-decker bus - killed 52 people and injured more than 700. Reviewing the video surveillance footage for London to try and piece together the events leading up to, during and after the bombings was a costly and labor intensive exercise. It highlighted a need for a process whereby the useful information could be retrieved much quicker.

Motion detection has been used in video surveillance for some time, offering the capability to focus attention only on those periods when motion has been captured. However, this is still often a lot of footage, primarily just showing people walking around a building for example, who are presenting no security threat. This leads to the adoption of technology which attached events or alarms to the video, tagging the video at the point when an alarm was recorded and developing an index of tags. With the increasing integration of different security disciplines, this means that an event or alarm generated by any of the systems can be tagged to the video. If, for example, somebody uses their access control card to enter a particularly sensitive area of the building, that event can be tagged with a piece of video. This can then be checked very quickly to ascertain if that person is the rightful carrier of the card.

This is again enhancing the intelligence of systems. No longer is it a case of saying ‘show me the video stream between 9am and 11am on Friday 11 May’. It is moving towards Google style searches, e.g. ‘show me the events where doors were forced’ or ‘show me the events when access control point A was entered’. In the age of the internet, we are very familiar with such searches and it enables useful and pertinent data to be identified much more quickly.

Forensic analysis: the next steps

Moving to the next stage and beyond just video surveillance, takes us into convergence again. By using multi-modal systems, the goal is to identify an event from all of the system inputs, including, for example, an intrusion into the IT network i.e. physical and IT security operating under a single front end control. Many so called cyber attacks can include a physical security element. One person could be orchestrating the attack remotely, from anywhere in the world, but often this will involve an accomplice operating in or close to the building, plugging in Ethernet cables, for example, or parked next to the building piggybacking on the Wi-Fi networks. By adopting fully integrated, multi-modal systems, you can have a much better level of situational awareness, knowing that not only is the network under attack but that it is being achieved through an Ethernet cable plugged into Rack 7 which was accessed via control point A.

Ultimately forensic analysis in this context is about very quickly finding the relevant information from the wide ranging and extensive data that is being processed, improving the speed of response and therefore the opportunity to resolve an incident. This area of research and development is seeing a lot of collaborative projects between security systems specialists and dedicated IT companies.

Illustrative examples

A few examples can show how integrated systems can provide a more holistic approach to safety and security which presents real and tangible benefits.

- Jack has to work in America for a few weeks and somebody uses his PKI card to enter a building in Switzerland. Thanks to the integration of the physical and IT security systems, an alert will be generated, either to security personnel, to Jack or to both.

- Erik is a successful salesman and has been head-hunted by a competitor. Before he leaves he decides it would be useful to his new company to have the customer data of his current employers. He attempts to download the data onto a USB stick but is prevented from doing so by a buddy system which requires an additional key from the sales manager.

Using myself as an example, I work out of an office in Zug in Switzerland but travel a lot and often need to work in our offices in Chennai in India. At Siemens we use a travel request system to book our flights and travel and we are currently looking at how we can integrate that with our security systems. If the system knows that I am in Chennai for 2 weeks, it should shut down my access to the Zug office, close down my Wi-Fi access in Zug and, because the IT systems know exactly where my laptop is connecting to the network, also shut down physical connectivity via Ethernet cables. Knowing when I am due in Chennai, all of my access protocols for the offices and IT connectivity can be activated for the 2 week period when I am there. If somebody attempts to enter my Zug office/use the network when I am not supposed to be there, an alert will be raised. There are also particular benefits here in terms of employee safety for those travelling to potentially dangerous countries. If the systems know that I am expected in an office in Iraq at 9.00am on 3 September 2012 and I have not been recorded by any of the access control system readers by 10.00am, an alert can be activated.

People sometimes raise concerns over the civil liberty issues of a ‘Big Brother’ society but these are clear demonstrations of how the technology can help to ensure greater safety and security for buildings, for the IT infrastructure and for people.

Future developments

With the increasing use of IP technology, particularly the advent of open standards enabling different systems to communicate more readily, so the distinction between the previously separate worlds of physical and IT security have become blurred. Convergence will only increase as security, along with other safety and building control systems, continues to migrate to the IT realm. A more holistic approach to safety and security is being adopted, one in which integration has a greater part to play. Systems are being developed which draw on a more structured and standardized approach using the IT networks but which allow greater flexibility in tailoring solutions to specific requirements. Data plays such an important role in the modern world that finding effective ways to protect it from the many threats, both those that currently exist and those that are yet to come, will become an ever increasing challenge.

Author

Mark Mooney, Head of Product Line Corporate Security, Siemens Building Technologies Division