Featured in this issue:

How secure is your building?

So-called smart buildings make use of networked technology to connect a broad range of systems to central management consoles for more efficient operation.

This use of networked technology has advantages for security as well, enabling feeds from security controls to be fed into the central management system so that anomalies in traffic flows can be seen and remedial action taken in an efficient, automated manner, as Colin Tankard of Digital Pathways explains. 

Full story on page 5…

The evolution of security intelligence

Threat landscapes have drastically changed from just a few years ago, with targeted attacks now common occurrences. As a result, many of today’s businesses have found themselves on the back foot.

Security intelligence offerings combining both Security Intelligence and Event Management (SIEM) solutions and ‘big data for security’ implementations are key tools for offsetting threats that result from both increased hacking, and vulnerabilities resulting from insider compromises, explains Sol Cates of Vormetric.

Full story on page 8…

Should the dark net be taken out?

Cybercrime in general appears to be on the rise, but despite the apparent success of the Operation Onymous sting at the end of 2014, law enforcement agencies still face problems when going after hidden websites on the dark net.

There are no international cyber-security laws, even though cybercrime tends to be global in nature. And the dark net is employed for both good and bad by criminals, journalists and political dissidents alike. So the big question in both ethical and privacy terms is would it really make sense to try and shut it down? Cath Everett finds out.

Full story on page 10…

More Snowden leaks reveal hacking by NSA and GCHQ against communications firm

Yet another batch of documents from the Edward Snowden leaks reveal that the US National Security Agency (NSA) and its UK counterpart, GCHQ, hacked Gemalto, a firm that specialises in security and communications products, including SIM cards for mobile phones.

What they were after were the private encryption keys to SIM cards, access to which would allow the agencies to eavesdrop – potentially on millions of people. Gemalto is headquartered in the Netherlands, but the attacks took place around the world.

The slides, published by The Intercept (http://bit.ly/1CZ1JLx), revealed the existence of a Mobile Handset Exploitation Team (MHET) and its operation Dapino Gamma. This targeted Continued on page 2…
How secure is your building?

Colin Tankard, Digital Pathways

Buildings today often incorporate the use of a building automation system, which provides automated centralised control of systems such as heating, ventilation, air conditioning and lighting. Buildings that employ such systems are often referred to as smart buildings. According to AutomatedBuildings, a smart building is defined as one that incorporates "the use of networked technology, embedded within architecture to monitor and control elements of the architecture for exchange of information between users, systems and buildings."¹

One survey from MarketsandMarkets forecasts that the market for smart buildings will grow from more than $4bn in 2013 to reach almost $19bn in 2018, the largest share of which will be commercial buildings.² The development of smart buildings is part of the fast-growing vision of the Internet of Things, in which all sorts of devices will increasingly be connected over IT-based networks, many of which will come into use in commercial buildings, offering smarter and more efficient data management to drive efficiencies. Gartner predicts that 26 billion devices will be connected and online by 2020.³

According to Memoori, the value of the Internet of Things in terms of buildings is as much about data as devices, as collecting data from more services and equipment will provide a more granular view of overall performance.⁴ For greater operational efficiency, such systems will increasingly collect, store and analyse data in the cloud.

**Smart buildings and security**

Commercial buildings and facilities face a range of security threats, including those from terrorist issues, disgruntled employees, workplace violence and criminal groups as well as from geopolitical actions such as riots and political unrest and natural disasters. There are also a number of other factors impacting building security that represent significant challenges. These stem from the nature of many commercial buildings, especially large complexes and high-rise buildings in dense urban environments that often are rented out to multiple companies. Security in such environments is complicated by the relative anonymity of users and occupants. This can lead to a poor security culture and result in interlopers going unnoticed and restricted movement in terms of elevators and lobby areas that can hinder guarding and emergency teams. The fact that services such as utilities tend to be grouped together into one service core, to make them easier to manage, can also make them easier to target.

"The largest application group within the smart building sector is for security, which will account for 47% of revenues by 2020, with controls such as alarms, CCTVs and access control systems becoming increasingly connected"

Because of factors such as these, monitoring systems are in widespread use in a range of facilities that include office buildings and complexes, industrial facilities and campus environments. Capabilities that they offer cover a wide range of physical scenarios, including perimeter protection, video surveillance,
**Minimum building security**

Building security measures should seek to provide:
- A consistent, compliant and auditable approach.
- Paperless environment.
- A strong secure perimeter with a limited number of access points into the building.
- Controlled access of all people and vehicles onto sites – maximising the benefits achievable from access control systems.
- Heightened security measures for areas containing particularly sensitive items and/or key operational equipment, documents, records etc.
- An intruder alarm system to support the physical security arrangements employed, supplemented, as appropriate, by CCTV cameras etc.
- Trained, knowledgeable security personnel where guarding needs to be deployed.
- Training of/communication with all building occupants and visitors to make them aware of security issues and the procedures that they are required to follow.
- Contingency plans and procedures in the event of security alerts and emergencies.
- Consistent and timely response from internal or external resources.
- Solid liaison and networking with appropriate external bodies, including police, fire service, ambulance service, local authority, utility providers and communication providers.


As buildings become more connected, one of the main challenges is managing the flow of data so that the current security environment can be understood and incidents can be responded to in an efficient manner based on gaining actionable intelligence from the data. This requires the use of a technology system that can collect, analyse and provide visibility into all information flows. This allows you to look for anomalies that could be indicative of a security risk, incident or vulnerability so that corrective action can be taken according to the incident response plan that has been developed in order to safeguard systems and applications.

For building controls, it is essential that security incident, logs and events are collected from both IT controls and physical security systems, such as logical and physical access control events, in order to give an overall picture of the environment and to provide visibility over what is happening in the network and in terms of physical monitoring measures.

For data protection purposes, all logs and events should be encrypted both in transit through the network and communications mechanisms, as well as in storage, where they should be held in a repository that is tamperproof and that is robustly protected with adequate access controls and granular, but not excessive, entitlements.

“All logs and events should be encrypted both in transit through the network and communications mechanisms, as well as in storage, where they should be held in a repository that is tamperproof and that is robustly protected”

Such a system must provide a central secure online environment that offers proactive task assignment and management for improving process flows, as well as providing a comprehensive audit and reporting facility. The audit trail is based on all events that have been tracked from multiple systems and should indicate what actions have been taken in response to every incident encountered. It also needs reporting capabilities that indicate the effectiveness of the measures that have been taken. This is also useful for governance purposes, such as alerting when security patches have not been applied in a timely manner so that remedial action can be taken.

**Effective controls**

Immediate action

So that senior executives can act on the information, reports should be provided as a dashboard, with information portrayed visually. This will allow those executives to analyse information and to pose questions to those in the organisation who can help lead to an overall improvement in security. It can also lead to more effective, granular policies being set, as well as achieving an easy to digest view of overall security, which is vital for effective governance, and for understanding the full range of threats faced and the effectiveness of incident response actions. Visualisation will also provide a spatial awareness of events, such as those surrounding the building as they unfold. Using such technology, it is possible to plot an incident on a map and apply additional information such as that...
available through Google Street View for a more visual description of the area. This provides a vital tool for remotely managing such an incident.

The central management system should also provide a facility for storing key documents or images relating to building protection that can aid in incident response, such as floor plans and standard operations procedures. This is also the place where best practices and procedures can be filed so that those in charge of responding to a particular incident can quickly find information that is relevant to dealing with, and recovering from, specific types of incident that could occur. And it is also where incident response plans such as fire and evacuation planning and incident management procedures and contacts should be stored. Currently, such information is typically lost in a cabinet on an inaccessible floor!

“Policies are only effective if all to whom they apply are aware of their responsibilities, understand what is expected of them and are made accountable for their actions”

The interface into the central management system should be web-based so that information is available over a browser interface and can be accessed from any Internet-enabled device, including smartphones and tablets.

By providing safe and secure interfaces to mobile devices or web browsers, remote access capabilities can be provided so that security operators can configure and control the system from wherever they are, and even out of hours. To gain full benefits, all components should be web-enabled, including the control panel, access control mechanisms and all monitoring capabilities. All endpoints that are external devices and are digitally controlled such as sensors, cameras, access control mechanisms, door and window locks should be included in the continuous monitoring process.

The central console provided by the security management system provides a policy enforcement point. Policies should be developed that cover every possible security scenario, based on detailed risk assessments that take into account the specifics of each building, its location, level of occupancy and type of business conducted on the premises. In developing risk assessments, it is important to take into account health and safety legislation compliance, which tends to vary from country to country. Policies are only effective if all to whom they apply are aware of their responsibilities, understand what is expected of them and are made accountable for their actions. Therefore, communicating with and training staff about the provisions of policies is essential.

Benefits

One of the benefits of using an IP-based security system is that a wide range of communications is supported, including call routing and mobile support, providing access to security-related information in a fast and efficient manner, making incident response quicker and more effective. Other communication methods can also be supported, including instant messaging and email for when information needs to be sent as text, such as sending floor plans to an onsite responder. These methods can also be used to send around mass notifications to all occupants or groups within a building — for example, to provide them with instructions or to send around warnings such as when a storm is approaching.

Overall, a security management system like this will improve the efficiency of building services and guarding teams by mitigating the risks that are faced and by providing for more effective and efficient remediation of incidents that occur.

Conclusions

A security management system for smart buildings will provide the underpinning for resilience in building management and critical systems, both for single or multiple buildings such as in a campus environment. For maximum effectiveness, it should cover all areas of risk that have been defined and should include mitigation strategies and automation for all security concerns identified. To suit the needs of particular buildings and facilities, the system should provide a choice of integrated applications and components to give facilities managers’ maximum flexibility in terms of risk mitigation and management. This will also avoid having to invest in components that are not required in a particular situation, providing for maximum return on investment.

By choosing a system that is IP-based, it can be more flexibly deployed and

Applications and information made available through the central console

The central console of a security management system should provide:

- Incident & crisis management log records and reporting tools.
- Audit records and reports.
- Standard operating procedures.
- Contact book.
- Technical security countermeasures, including alerts and real-time change processes and workflow.
- Business continuity plans.
- Health and safety records.
- Investigations support.
- Risk assessments.
- Floor plans.
- Best practices and procedures for bomb threats and suicide bombers, hostile reconnaissance, lift entrapment, suspect packages, protest/occupation/civil unrest, lost/stolen/ found property, workplace violence, active shooter, datacentre security, critical alarms, mail room procedures, CBRN (chemical, biological, radiological and nuclear warfare)/HAZMAT (hazardous materials and items) and domestic extremism.

The evolution of security intelligence

Sol Cates, Vormetric

Threat landscapes have drastically changed from just a few years ago with targeted attacks now common occurrences. Hackers are actively seeking to steal credit card data, personally identifiable information (PII), critical intellectual property (IP), and other legally protected information to retail to the highest bidder. As a result, many of today’s businesses have found themselves on the back foot.

Furthermore, nation state-motivated attacks on both business and government entities are escalating, with critical intellectual property in the form of plans, formulas, production methods and the reputation of national institutions the primary target.

Expanding the periphery

At the same time, organisations are expanding their periphery beyond the traditional enterprise WAN and firewall – SaaS applications now account for over 50% of IT application spending, according to Gartner, and spending increases by both government and commercial enterprises of all cloud resources is forecast to nearly double by 2018. Mobile usage of enterprise data is also expanding, and a key concern for many organisations. Not to mention the avalanche of data starting to flow form the Internet of things (IoT) as new devices like cameras, refrigerators, home security systems, automobile sensors, power grid data and extended location information connect up to the Internet.

This expansion in the use of new technologies, combined with the increased threat environment as ‘dark’ sites expand to support a new international criminal class, is driving the need for tools that can sift through data to intelligently and proactively identify threats in process before they compromise organisations.

Representative of what is turning into a multi-billion dollar industry, organised criminal gangs are putting much more time, energy and resources into identify-

Key benefits

The main benefits of an integrated security management system include:

- Operational excellence model.
- Risk and gap analysis.
- Real-time audit and process flow.
- Paperless and prompt decision-making.
- Accountable actions.
- Real-time change management.
- Improved productivity resulting in commercial advantage.

Source: Global Aware International.

reduces the need for deploying physical communication interfaces such as cabling that are limited in their range. With an IP-based system, controls such as wireless intrusion detection units can be placed on each floor, connected via Ethernet or wireless, reducing the cost involved in implementing physical connections and improving overall security by being able to centrally control all devices.

As well as providing benefits for facility managers, a web-based security management system will improve the perception of security among occupants, making them feel safer, thus making prospective tenants more likely to be interested in taking space in the building. However, in order for this sense of security to be felt, all occupants should be made aware of the protection measures that are being taken so that they buy into the schemes and can achieve peace of mind.

About the author

Colin T ankard is managing director of data security company Digital Pathways (http://digpath.co.uk), specialists in the design, implementation and management of systems that ensure the security of all data whether at rest within the network, on a mobile device, in storage or data in transit across public or private networks.

References