SECURITY
The e-Brief
telecomasia

Sponsored By

CISCO

www.telecomasia.net

telecomasia

QUESTEX MEDIA

MAIN STORY

Collaboration, control and intelligence key to combating threats

Service providers must develop new integrated threat-centric responses for tackling increasingly sophisticated attacks

Lachlan Colquhoun

Organizations around the world, many of them leading service providers, are spending significant resources to combat cyber-attacks, and yet the number of attacks continues to rise.

A recent study by the Ponemon Institute found that the average cost for a data breach has grown to $4 million, representing a 29% increase since 2013.

The longer it takes to detect a data breach, the more expensive it becomes. Breaches which were identified in less than 100 days cost companies an average of $3.23 million, while breaches found after the 100 day point cost an additional $1 million, or an average of $4.38 million.

Threats are also continuing to increase in both volume and sophistication, with recorded attacks up 64% in 2015.

Soon, the developing world of the Internet of Things (IoT) will create new vulnerabilities for the telecommunications sector to grapple with. Gartner estimates that 6.4 billion devices and objects are connected to the internet in 2016, a number that will rise to 20.8 billion by 2020. This will give cyber attackers three times as many targets, as well as new attack vectors to pursue.

Communications service providers are already feeling the impact of the vulnerability of the IoT, with Germany's Deutsche Telekom attributing a recent outage affecting millions of its broadband customers on a failed malware attack linked to the Mirai IoT botnet.

Service outages in fact continue to occur regularly worldwide due to a variety of causes. These can cause massive disruption to customers all across the spectrum from individual home users to the biggest corporates.

Service providers also have to deal with unique threats such as attacks on their infrastructure and applications by government agencies seeking to establish covert surveillance, according to a recent report from Deloitte.

As the telecoms industry is undergoing digital transformation and moving toward a more digital future, telecoms service providers will very likely encounter entirely new types of cybersecurity risks to data, applications and networks.

UK mobile operator 3, for example, reportedly became the latest victim of a major telco cyber-security breach, with one of its databases, containing the details of up to six million customers, being hacked via an employee login.

As such, security is the number one priority for many service providers and enterprises in dealing with changing and sophisticated threat landscape.

Time to respond makes the difference

Cisco's 2016 Midyear Security Report also highlights a crucial point observed by the company's Security Team: detection is not enough – time to detect as a key metric is crucial in the mitigation of data breaches/compromise.

The Ponemon research found the average time to identify a breach was estimated at 201 days, and the average time to contain a breach was estimated at 70 days. Increases and decreases in Time to Detection (TTD) over this period highlight the ongoing and heated "arms race" between attackers and defenders, occurring as the digital world continues to expand.

This is a significant issue for the many organizations currently working with legacy technology, which typically delivers security alerts – and not responses – when breaches are detected.

There is also a reliance on point solutions and a "triage" approach of dealing with threats on an incident by incident basis, when a holistic and strategic approach should be the foundation for response.

In response to growing awareness that detecting and responding to breaches as rapidly as possible is essential, security vendors are increasingly developing solutions that are automated, and able to respond immediately upon detection.

Cisco has been able to reduce its median TTD to about 13 hours, well below the current industry estimate of 100 to 200 days.

But a timely response isn't just important when an attack has been detected. The Cisco Midyear Report picks up on this issue, noting that even though patches are available from major software vendors when vulnerabilities are announced, many users are slow to test and install these patches.

This creates a gap between the availability and the actual implementation of the patches, giving attackers ample time to launch their attacks. The faster a vulnerability is patched, the less time an organization is exposed.

Human resources alone are not enough

Internal security staff are an important component of any organization's response to the evolving threat landscape. But

www.telecomasia.net

telecomasia
QUESTEX MEDIA

according to the 2015 ISACA Global Cybersecurity Status Report, 86% of respondents believe there is a shortage of skilled cybersecurity experts, and among organizations planning to hire more security staff, 92% said it would be difficult to find skilled candidates.

More recently, ISACA's Cybersecurity Jobs Index found that 27% of organizations need six months to fill a cybersecurity position, up from 24% in 2014.

Rigorous approaches to governance and staff training and education are critical to addressing this skills gap.

But training staff on procedures and increasing the number of security professionals may not be enough to redress the balance, given the prevalence and the nature of emerging attacks, many of which are automated and require an automated response.

Service providers and other organizations are turning to technology to deliver the required response, using encryption and sandboxing technologies to protect data from intrusions, and ultimately from data losses. Sandboxing is often used as a defense against email-borne threats, and offers an isolated environment where suspicious code can be tested and observed.

Encryption is a most effective way of protecting data, but just under half of all online traffic is encrypted, partly due to issues around authentication.

Collaboration is key

Another way service providers must respond to the evolving threat environment is by learning to collaborate more closely and share intelligence about threats.

In an interconnected world, organizations are collaborating with each other as never before. In the world of digital disruption new companies are leveraging the technology of incumbents, with telecoms players and service providers at the core.

The reality is that these new commercial ecosystems are built on the rapid exchange of increasingly large volumes of data. But if this new digital world is to deliver on its promise, trust needs to be maintained, which will require vigilance on behalf of security professionals.

A key to collaboration is the idea of threat sharing to coordinate an effective response, both strategically and tactically.

Many professionals are sharing industry specific intelligence through Information Sharing and Analysis Centers (ISACs).

Service providers must also work with IT or outside security experts to quickly identify the sources of breaches, and stop the most sophisticated attack methods.

Disclosure is a vital element not only of transparency, but also threat sharing. Regulators in Asia are waking up to this fact, and are developing new regimes requiring mandatory disclosure of breaches.

The reality is that today, the attackers are outpacing the capacity of service providers to respond.

This has created a context where a new generation of solutions and a new approach to collaboration and threat sharing by the defender community is required.

Leveraging best of breed solutions from security specialists, and working with them on tailoring the response strategy presents as a first step, and many service providers are taking this initiative. ●

www.telecomasia.net

telecomasia
QUESTEX MEDIA

Forrester: Security to temper IoT growth in 2017

Interest in the Internet of things (IoT) hit a fever pitch in 2016 but technologies and use cases for the IoT are wildly divergent. No a single one of these leads to dramatic adoption, considering that IoT is an amalgamation of specific use cases and technology.

Thus, IoT's potential to fuel business growth is accompanied by multifaceted complexity. CIOs recognize that the IoT holds the promise to enhance customer relationships and help them drive business growth. However, it's a complex undertaking that affects business strategy and nearly every role in the CIO's organization.

Also, IoT adds more fuel to the security fire, so it represents a two-pronged threat in 2017. It may potentially expose businesses to breaches, and hackers could turn IoT devices themselves into distributed denial-of-service (DDoS) weapons.

Forrester Research predicts that IoT technology and architecture will emerge to aid insights and scale in 2017. The IoT will be distributed across edge and cloud, boosted by AI and containers; prototypes of smart contracts built on blockchain will appear; and vendors will offer a dizzying array of tech to support IoT field use cases.

Moreover, IoT security will steamroll into the public eye. Most IoT devices run on embedded Linux and utilize open source components, vastly increasing attack surfaces, the research firm says.

Many IoT solutions also lack simple patching mechanisms, making addressing security vulnerabilities challenging.

Forrester predicts that there will be a large-scale IoT security breach next year, and hackers will continue to use IoT devices to promulgate DDoS attacks. ●

PwC: Firms adopt innovative safeguards to manage threats

Many organizations no longer view cybersecurity as a barrier to change or an IT cost, understanding that cybersecurity solutions can also facilitate growth, create market advantages and build trust.

This shift in thinking is mostly an outgrowth of the digitization process, says the Global State of Information Security Survey 2017 by PwC.

Data privacy and trust have also become critical business requirements as exponentially more consumer and business information is generated and shared.

Forward-thinking organizations are pivoting toward a new cybersecurity model capable of acting on analytic inputs and adapting to evolving threats. Underpinning this approach are solutions like real-time data analytics, managed security services, advanced authentications and open-source software, the survey adds.

If there is one unifying thread, it's the cloud - the power and interoperability of the cloud enable organizations to use a range of synergistic technologies. The simplification of cloud architectures can also help build secure products and services.

Cloud-integrated solutions can also enhance data privacy capabilities – a necessity as consumers and governments become more privacy-aware.

Sophisticated technologies can mitigate the impact of attacks, but threat actors will likely remain ahead of the game by developing new circumvention tactics. Organizations that hew to the fundamentals — employee training, up-to-date policies and controls, and a commitment to readiness and resilience — will be better prepared. ●

www.telecomasia.net

telecomasia

QUESTEX MEDIA

Safeguard your networks against cyber attacks

Proactive threat hunting and frontline defense allow telcos to control and minimize the overall risk from cyber attacks to their networks

Recent cybersecurity reports show that the threat landscape is evolving and shifting for telecoms service providers and the industry as a whole. Yet an unprecedented increase in cyber attacks, coupled with an ever growing talent shortage, has put service providers in hard to defend positions. Rather than wait for the adversary to strike, service providers should take a more proactive approach by working with experts to track and eliminate cyber adversaries from their networks as early as possible.

Proactive threat hunting

The Cisco Security Incident Response Services (CSIRS) Team is a specialist threat hunting resource which works with an organization to design a custom plan. The plan acts to define the scope of the engagement, identify coverage and gaps in visibility, deploy the needed technology required for full visibility, assess the environment leveraging the latest intelligence, analyze findings, and provide a final report of both findings and prioritized recommendations. CSIRS can also lead or assist in the response to any and all findings during the course of the compromise assessment.

CSIRS creates the following values:

- Stronger security posture through an approach that proactively hunts for and addresses unknown issues
- Higher confidence in what is actually happening in your network, including greater visibility and deeper understanding of organization operations and infrastructure
- Access to skilled incident responders with years of experience dealing with numerous types of incidents
- Full access to Cisco's tool suite (AMP for Endpoints, FirePOWER NGIPS, Stealthwatch, Umbrella, and more) during the incident, to provide greater visibility, speed and a broader understanding of all threats in the network

Different threats require different responses

Each organization, threat, risk tolerance, and incident all combine to create a unique situation that requires a tailored approach to resolution. Starting with an initial kick-off call to triage the current situation, the CSIRS Team will first work with the service provider to determine what can be done quickly to contain the situation.

Within 24 hours, Cisco will then have experts onsite, serving as liaison back to the larger CSIRS Team working to bring the full muscle of Cisco to combat the issues.

Value of frontline defense

Protection before, during, and after an attack

Today's security appliances and agents must wait until malware reaches the perimeter or endpoint before they can detect or prevent it.

www.telecomasia.net
telecomasia
QUESTEX MEDIA

VENDOR VIEWPOINT

Attacks have many phases—before it is launched, the attacker needs to stage internet infrastructure to support each phase. Two early phases are to redirect/link to a malicious Web domain or send a malicious email attachment. For the former, most attacks leverage exploit kits (e.g. Angler) as the first stage before dropping the final payload.

Attacks that target organizations often leverage email attachments or direct payload downloads. Yet attacks with an objective to exfiltrate data, still must initiate a command & control callback.

In order to identify where these domains and other Internet infrastructures are staged, the best frontline defense point is to enforce security at the DNS and IP layers over any port.

Front line defense adoption with Cisco Umbrella protects against attacks earlier in the kill chain. Enforcing security at the DNS layer prevents a malicious IP connection from ever being established or a malicious file from ever being downloaded. This same DNS layer of network security can contain malware and any compromised system from exfiltrating data. Command & control callbacks to the attacker's botnet infrastructure are blocked over any port or protocol. Unlike appliances, the cloud service protects devices both on and off the corporate network. Unlike agents, the DNS layer protects every device connected to the network—even IoT. It is the easiest and fastest layer of security to deploy everywhere.

Cisco Umbrella comes with two modules which provide security policy enforcement over internet traffic of subscriber as well an investigation tools for the enterprise security expert to get firsthand information on threat in the network.

Addressing the malware threat

With the rise of polymorphic malware and it's no secret that today's advanced attackers have the resources, expertise and persistence to compromise any service provider at any time. Service providers face tens of thousands of new malware samples per hour and attackers can rely on simple malware tools to successfully compromise a device. Traditional defenses, including firewalls and endpoint protection, are no longer effective against these attacks, the blacklist approach of matching a file to signatures of known bad malware no longer scales to keep pace and newer detection techniques, like sandboxing, are not 100% effective.

No security control can live in a vacuum. In order to defend against advanced malware, significant coordination is required between the defenses on the network, the protections on the endpoint and the management console tracking threats and remediation activities.

Cisco has taken a more comprehensive approach to address these challenges in detecting malware. Enabled by a customer base of thousands of global enterprises and millions of endpoint malware protection agents in use, Sourcefire collects millions of malware samples every month. Tens of thousands of software attributes are analyzed within Cisco Talos threat intelligence cloud to separate malware from benign software. Network traffic characteristics are also analyzed to identify malware searching for CnC networks. It also leverages its vast installed base to determine what normal file and network activity looks like, both globally and within each specific customer organization, for comparison.

Please visit http://www.cisco.com/go/security for more information about Cisco security solution. ●

www.telecomasia.net

telecomasia
QUESTEX MEDIA