Government Business Council

vmware

carahsoft.

The Call from the Basement

Combating Insider Threats in State & Local Government

With its immense trove of official emails, city payroll files, confidential police documents, and inmate records, San Francisco's FiberWAN data system forms the backbone of local government IT operations – and for a brief period in the summer of 2008, the city was left virtually helpless when a disgruntled employee hijacked the network, reset administrative passwords, and effectively locked out all system access. While Terry Childs, a former city network administrator, was eventually taken into custody and charged with computer tampering, the potential ramifications of his actions stunned San Francisco. As one city official noted, "He had the trump card, and he could have brought everything down if he wanted to."[1]

The FiberWAN breach is only one incident in a rapidly growing list of public sector cyber attacks – since then, state and local governments have been targeted by an onslaught of network and data breaches. In the face of these increasingly sophisticated intrusions, IT leaders are redoubling efforts to construct resilient defensive measures. However, when it comes to cybersecurity, focusing solely on external threats isn't enough. If organizations are to successfully protect critical data and infrastructure, they need to account for the full destructive potential of insider threats – the call coming from the basement.

Motivations & Methods

The case of Terry Childs represents an extreme example of insider threat, but not all internal breaches follow the same formula. Insider threats – defined broadly as any current or former employee, contractor, or industry partner whose actions negatively impact organizational data, information systems, or networks – can be either intentional or unintentional.[2] Malicious insiders deliberately acting against an organization's interests may be motivated by a variety of incentives: retribution, financial gain, espionage, and so on.[3] However, cyber breaches often manifest themselves in more mundane forms than premeditated sabotage, fraud, or information theft; the majority of them, in fact, are the result of simple human fallibility. These unintentional insider threats stem primarily from four different channels:[4]

Accidental disclosure – sensitive information posted publicly, mishandled, or communicated to the wrong party

Malicious code – electronic entry into networks or systems acquired through social engineering schemes (e.g., phishing/spear phishing, planted or unauthorized USB drives) and carried out via mal-ware or spyware

Improper handling of physical records – lost, discarded, or stolen non-electronic records

Misplaced data storage devices – lost, discarded, or stolen data storage devices (e.g., laptops, mobile devices)

Public sector leaders are growing steadily more concerned about the threat that exploited or careless insiders pose to organization cybersecurity. In a 2014 study, 80 percent of state Chief Information Security Officers (CISOs) predicted that the next year would see a rise in pharming and phishing scams; moreover, while CISOs alluded to a plethora of increasingly sophisticated threats, malicious code continued to top their list of most potentially dangerous attack vectors.[5]

Detection & Prevention

While efforts to build up defensive measures are often hampered by budget constraints – state CISOs cite insufficient funding as the top obstacle to more effective cybersecurity[6] – integrating proactive policies and consistently following best practices can help to substantially reduce insider threats. On the technical side, organizations can better enforce privileged user access to sensitive information by implementing strict identity and access management, multi-factor authentication, and partitioned networks with separate security domains.[7] In addition, automating processes allows organizations to ensure compliance and expedite incident response,[8] while predetermining backup and recovery processes can aid cybersecurity teams in timely damage assessment and containment.[9]

State and local organizations can also avoid exposing themselves to internal breaches by incorporating techniques focused on human error mitigation and factoring insider threats into risk assessments. At the hiring stage, managers can screen for potentially threatening behavior through comprehensive background and reference checks, and organizations can also provide security training on insider threat recognition and general cyber hygiene in order to promote greater employee risk awareness. Furthermore, organizations might consider monitoring and controlling remote access in order to enforce threat-resistant workplace mobility.[10]

Looking Ahead

The past several years have seen an explosion of cyber attacks across the public sector, and state and local governments are increasingly aware of the corresponding need to manage vulnerabilities and preserve the integrity of critical data and network infrastructure. However, eye-catching media headlines detailing the cyber exploits of hacktivists and foreign governments only tell half the story – when it comes to data breaches, the most significant perils may come from the within the organization itself. As state and local leaders continue to map out proactive, cohesive cybersecurity strategies, it is crucial that they take into account both technical security capabilities and the human factor of risk mitigation in order to successfully predict, assess, and combat the growing insider threat.

Sources

1. "San Francisco Admin Charged with Hijacking City's Network." http://www.wired.com/2008/07/sf-city-charged/
2. "Anticipating and Solving the Nation's Cybersecurity Challenges." https://resources.sei.cmu.edu/asset_files/Brochure/2014_015_001_91730.pdf
3. "Malicious Insider Threats Greater Than Most IT Executives Think." http://www.computereconomics.com/article.cfm?id=1537
4. "Unintentional Insider Threats: A Foundational Study." http://www.sei.cmu.edu/reports/13tn022.pdf
5. "2014 Deloitte-NASCIO Cybersecurity Study." http://www.nascio.org/Publications/ArtMID/485/ArticleID/85/2014-Deloitte-NASCIO-Cybersecurity-Study-State-governments-at-risk-Time-to-Move-Forward
6. "2014 Deloitte-NASCIO Cybersecurity Study." http://www.nascio.org/Publications/ArtMID/485/ArticleID/85/2014-Deloitte-NASCIO-Cybersecurity-Study-State-governments-at-risk-Time-to-Move-Forward
7. "Anticipating and Solving the Nation's Cybersecurity Challenges." https://resources.sei.cmu.edu/asset_files/Brochure/2014_015_001_91730.pdf
8. "NIST Computer Security Incident Handling Guide." http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
9. "Anticipating and Solving the Nation's Cybersecurity Challenges." https://resources.sei.cmu.edu/asset_files/Brochure/2014_015_001_91730.pdf
10. "Anticipating and Solving the Nation's Cybersecurity Challenges." https://resources.sei.cmu.edu/asset_files/Brochure/2014_015_001_91730.pdf

About Carahsoft

Carahsoft is the trusted Government IT solutions provider supporting a vast partner ecosystem of manufacturers, channel partners, systems integrators, and service providers committed to serving the public sector. Carahsoft is the largest VMware Government Aggregator and Distributor and offers the full suite of VMware products and services through our channel partners leveraging many SLED contracts.

About GBC

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight and analytical independence. As an extension of *Government Executive*'s 40 years of exemplary editorial standards and a commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis. Learn more at www.govexec.com/insights.