THE HUMAN INSIDE

The Human Inside

Facing the Growing Cyber Threat of Third-Party Access

The era of believing in the impenetrable armor of cyber defense is over. We are flooded on a daily basis by headlines of major computer breaches compromising millions of consumers' private information. Through our daily contact with computerized systems, the public is left defenseless by the network vulnerabilities of the companies' they do business with. Outside attacks from organized crime and nation-states remain our focus but another adversary is beginning to surface that is even more insidious – the insider.

While plenty of insider breaches occur due to employees' lack of awareness of their company security policies and basic online safety practices, a significant number of incidents stems from the malicious insider. According to Forrester's "Understand the State of Data Security and Privacy" report, that number of information compromises by malicious insiders reached 25% in 2013.

Intentional or not, the employees' access to critical assets on an enterprise network significantly raises a company's risk of being compromised in a way that evades perimeter detection. It only takes a flash drive, a personal email, a click on the wrong link, or access the cloud and, voila, company secrets are lost. Furthermore, allowing network access to contractors and partner organizations open the gates to third party access that becomes a headache to control.

Today's dynamic cyber environment offers another layer of challenge that threatens to obliterate the way companies normally handle security and put added pressure on the CISO's shoulders – the growing ubiquity of mobile and the BYOD (Bring Your Own Device) policy shift. As more employees and contractors take their work home and access networks with their smart phones or personal computers on the go, the risk of vulnerability rises exponentially. The upsurge of devices with Internet connectivity makes it easier for hackers to wreck havoc from hidden locales. Simultaneously, many corporations struggle to keep up not only with the sophistication of malware and APTs but also implementing company policies aimed at preventing such attacks. The question arises, how can a company prepare itself for third-party access that is rising across enterprises as partners, contractors, clouds and BYOD policies enter the picture?

"More and more people work from remote locations these days, which is especially the case with large enterprises that hire international contract teams," says Guy Thier, the CIO of Arbonne. "The challenge we face is dealing with new devices that have access to our network is not to be taken lightly. Every phone, tablet and laptop becomes the network endpoint giving the bad guys a phenomenal opportunity to enter."

Shifting Focus from Tactics to Strategy

Arbonne is one of many companies that are attempting to expand their focus from heavily guarding the perimeter to include strengthening the systems' detection capabilities. But to move resources from a pre-architected area of known threats to the dark depths inside network's protective walls where stealthy attackers hide, is not easy. "It is hard to see the risk there until it is too late," says Kirsten Bay, the CEO of Cyber adAPT, a start up company on an aggressive mission to not only provide enterprise detection solutions to spot the intruders before serious damage occurs, but also to educate the public and corporate boards about security's impact on the entire business. According to Bay, boards are not concerned with individual tactics attackers use to break into their networks, but, rather, the impact on the enterprise by attackers. Therefore, the discussion gains merit at the risk level – understanding how security will impact the company's bottom line and the decisions that will need to be made to properly assess and protect critical assets. "Cyber security is at a tipping point; it's a crisis. We need to change our approach and quickly," she adds. "But before we do so, we need to change our understanding and ability to articulate the message to the top."

In light of recently publicized breaches, the discussion of security and risk models have entered the boardroom. The issue is starting to be taken more seriously, especially as more players enter the arena in the form of "trusted outsiders" connecting to the networks as dependable insiders allowing their laptops and smartphones to circumvent carefully placed firewalls. But while the conversations have become more heated, the problems aren't new, only more visible. Untangling spaghetti-like systems to look for vulnerabilities that need protection and fortification can be as challenging as being able to effectively present the criticality of the threat to boards whose primary concern deals with business growth and funneling resources to places that can maximize returns.

"Boardrooms are only now becoming aware that cyber security is a corporate governance issue at the highest level but aren't sure exactly where it fits in their discussion and their strategy," adds Bay. "It therefore becomes very helpful for organizations to first be able to validate and monitor whether a third-party isn't opening security holes."

WHILE MASSIVE CHANGES HAVE OCCURED IN THE USE OF INTERNET PROTOCOLS, NOT MUCH HAS CHANGED IN THE LAST 20 YEARS IN SECURITY STARATEGY

Shining Light in Dark Corners

If we are to shine a light into the darkness to clearly see which threats are realizing our security fears, it is imperative we better understand the current state of security to gauge the sophistication of adversaries. Cyber security is still in its infancy. While massive changes have occurred in the use of Internet protocols, not much has changed in the last 20 years in security strategy. Even the methods of attacks have changed little. What has evolved are the tactics used to exploit vulnerabilities, making them more difficult to catch. But the fundamental approach to our security defenses has not been developed with the same kind of rigor and urgency. The focus continues to remain on perimeter defense, further missing the point. Rather than zeroing in on the strategies that underlie attacks, companies still spend more time and effort dwelling on surface tactics. Meanwhile, increasing number of networks get successfully attacked every day. As John Chambers recently shared, "There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked."

Having many "eyes on the glass" monitoring logs and network traffic it is no longer sufficient when people are increasingly shifting locations and crossing security thresholds. Companies can no longer afford or risk missing a spike on an alert gauge, but are at constant challenged by the massive onslaught of attacks each second and a scarcity of the specialized and expensive labor force needed to fight the adversary. "It is imperative that businesses find a way to automate the processes, if they are to scale into true 'active defense'," says Scott Millis, CTO of Cyber adAPT. According to Millis, everyone's life would be significantly improved if the network sentinels had the ability to turn on and off specific protocols to detect malicious intrusion without human intervention to have the ability to detect malicious intrusion. "What's desperately needed is the night watchman inside the network keeping an eye the crown jewels."

Customer Sentiment Embraces Security

While protecting the network is at the core of maintaining the corporate sense of safety and dependability among employees, the importance of this sentiment extends well beyond the corporate walls. No one knows exactly by how much attacks and compromises against digital information have increased, but we do know that the attacks are becoming more public and viewed as significantly more threatening at a personal level. As such, developing an integration strategy where the enterprise networks are safeguarded along with customer relationship management and legal considerations.

"Our customers feel more at ease, knowing that we are doing everything we can to protect their personal information," says Thier. "In the case of security, the lines between corporate and customer are more prone to blur. Their security and our security are now one and the same."

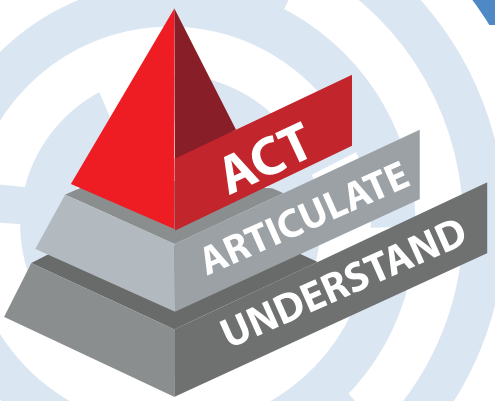
The latest consumer focused company breaches and subsequent release of consumer personal information has created a tipping point for highlighting the importance of cyber security, but the industry, and businesses, aren't sure yet how to action on making substantive changes. Most organizations are still wrapped up in building higher walls, placing armed soldiers at the borders, in general - bringing their defenses up. They have neglected the watchmen in the streets behind the wall to guard against the "inside man" as well as infiltration that has already penetrated the walls undetected.

"What's desperately needed is the night watchman inside the network keeping an eye on the crown jewels."

-Scott Millis, CTO, Cyber adAPT

Thus, every person in charge of cyber defense strategy is faced with a multi-pronged challenge:

1.To intimately understand the capacity and gaps of their security infrastructure against the evolving capabilities of their opponents, which includes the strength of their perimeter defense.



2.To understand the vulnerability of their most critical assets and know the kind of solutions needed to in order to fill those gaps. Articulate the need for a new approach to the board members who often don't under the gravity of the situation until after the damage is done.

3. To take more proactive role in defending those assets by increasing their monitoring and detection power to help identify malicious threats before they damage the organization.

The misuse of data by employees, whether intentional or not, is not going to go away, nor will vulnerabilities of accessing corporate networks from remote locations. What clearly needs to change is company's top down understanding of risks associated with a reactive approach and bottom up articulation of those battling the adversaries. Only when managers win the board's support in changing a security strategy, will the actions taken start shifting the dynamic of the ecosystem by illuminating it from the inside.

Headquarters
337 Mirada Road, Second Floor
Half Moon Bay, CA 94019

Dallas Location
14755 Preston Road, Suite 405
Dallas, TX 75254

Chicago Location
135 Park Avenue, Suite 201A
Barrington, IL 60010

Email
info@cyberadapt.com