4 Fallacies around Security Breaches to Consider for 2017 Budget

The cyber security landscape changes quickly and planning your 2017 investment strategy may be something you are iterating right now. Security officers responsible for investment decisions rely on policy portfolios and tactical shifts, but also tend to be drawn to security trending topics and industry buzz. We are constantly being fed by over simplified market terms such as big-data, cloud security, UEBA, security analytics, IOC, and many more, so this makes it difficult to identify truly important developments.. The current state of world for enterprise cyber defenders is clearly perilous and likely to keep cybersecurity at the top of every corporate agenda.. So, how can security leaders bridge the gap between the current state and future desired state of protection with careful 2017 investments in security infrastructure? What should leaders keep in mind when choosing the next areas for investments? Lets examine 4 fallacies that will need to be avoided in order to build a better 2017 plan for security risk reduction and improved efficiency.

Fallacy #1: Better security means deploying more prevention measures

The reality: Many security vendors are doing their best effort to stop attackers at the gate; unfortunately they are far from providing security teams with a silver bullet. This perimeter-centric approach is long obsolete. The reality today is that most organizations are being breached one way or another. Even mature, well-funded organizations which invest millions in cyber security end up in the business news as victims of a major breach. This is why it was no surprise to see Gartner predict that by 2020, 60 percent of enterprise information security budgets will be allocated for rapid detection and response, up from less than 30 percent in 2016.

Fallacy #2: Breach is inevitable, so following regulations will be sufficient

The reality: Attackers are always moving much faster than regulators! It is no longer enough to be compliant with regulatory requirements such PCI DSS and HIPAA to stop network downtime due to a ransomware attack. Successful attacks are indeed inevitable, yet security breaches could have been mitigated by responding to incidents in time. While every organization may expect a compromise, the key question is how fast the security team reacts once the attacker has crossed the first perimeter. The longer it takes to respond, there will be a greater risk of irreversible damage and the greater the liability exposure. Security alerts should be reviewed and once validated as real threats, a detailed investigation must be performed quickly in order to effectively mitigate the incident before it becomes a full-blown breach.

Fallacy #3: We can rely on our SIEM for performing security investigations

The reality: SIEM is a great tool to provide high-level details on security events and is important in order to prioritize what should be investigated, but trying to understand if the threat is real through log data is rarely enough. SIEM can point us where & what to investigate, but it’s not an investigation platform since it is missing the actual data. Security teams should be able to understand when data was accessed, by whom, where it traveled to, and what was in it. To streamline security investigations, organizations must augment their SIEM with advanced forensics tools so that security professionals could make faster and more informed decisions based on the actual content of network conversations, rather than just the metadata.

Fallacy #4: We need a team of dedicated experts to do network forensics

The reality: Let’s face it; the skillset gap in security staff is a problem. The entire cybersecurity industry is suffering from a lack of specialized education and training. Most of today’s forensics solutions require advanced skill-sets that are very rare. This is why a key evaluation factor when choosing a forensics tool should be usability, which empowers your existing team without requiring additional resources. Your network forensics platform should be able to do all the heavy lifting of data analysis, providing security teams with intelligence that is human-readable and introducing workflows that are driven by automation. Bottom line - Your forensics platform should help the entire security team explore the data and conduct investigations in less time while using fewer resources.

About WireX Systems

WireX Systems is a network forensics company that has shifted the paradigm in security investigations. Using Contextual Capture™ technology, the solution continuously translates network traffic into comprehensive intelligence that can be immediately understood and expands forensics history from days to months. Today, leading enterprises choose WireX Systems as a key component in their security infrastructure to accelerate incident response, mitigate data theft and simplify responding to the magnitude of security alerts they must action on a daily basis.