OrbusSoftware

How to Survive A Cyberattack

The internet and cybercrime practically walk hand-in-hand; as the internet grows and encompasses more of daily life, so malicious actors gain more weak points to attack, and more sophisticated methods. Most recently, attackers were able to gain access to US government data not through a direct assault, but by targeting their software supply chain, hitting software firm SolarWinds. It is no longer a question of if an organization will come under attack, but when. How can firms protect themselves and deal with the fallout? And how should Risk professionals and enterprise architects adjust in the face of this new challenge?

The Sunburst Hack

The attack on SolarWinds itself took place in early 2020, but details have only recently come to light, and the exploit is known as Sunburst. The hack that took place is known as a 'supply chain attack', wherein hackers target vulnerabilities in the targets supply chain. As SolarWinds software is widely used by governments and large organizations around the world, such an attack could hit a wide variety of potential targets. Believed to be the work of a government-backed cyber hacking team, the hackers were able to gain access to sensitive government information from the US and many other countries around the world. It is believed to be one of the worst cyber-espionage incidents the US government has ever experienced, in part due to the length of time that that attack went unnoticed – 8 to 9 months.

The point of attack came from a typically harmless vector, an automatic software update for SolarWinds' Orion product that had been compromised and contained malicious code. In fact, to gain access to Orion, the hackers used another supply chain attack, targeting Microsoft, which in turn allowed them access to SolarWinds. Once the update was installed by an unsuspecting user, the malware would execute, remaining dormant for a short period before communicating with the attackers and granting backdoor access.

Most of the details aren't particularly relevant to organizations. Attacks happen, and sometimes they're successful; that's just one of the many prices of doing business. However, there are several notable factors which make this a more worrying development:

Growth of Government & Corporate sponsored hacking

The Sunburst hack is yet another in the growing list of examples of national governments becoming directly involved in cyber attacks. Though corporate-led espionage has not had any such high profile stories, there is little doubt that attacks on competitors are a growing problem as well. All of which will contribute to more resources, more frequent attacks, and a wider variety of targets as cyber hacking escalates into cyber warfare.

Interconnected Supply Chains

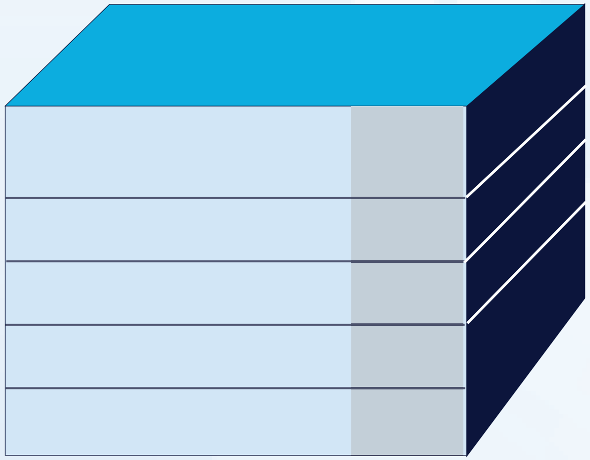
Perhaps the most worrying aspect of the Sunburst hack was the method. The modern business world has never been more interconnected, which opens up many more companies as potential targets. What is more, even if an organization is not a target of a hack, supply chain attacks by their nature can end up catching many in their net; the Sunburst hack was only used against a fraction of the infected, for example. Some might speculate that there are still only a handful of potential targets in the software space, and most of these organizations will already have strong protections against cyber attacks. But this ignores the spread of internet connections. Could, for example, Mazda become a target? If a government agency uses Mazda cars, then the car's OS could be a target. What about a consumer goods firm, like Whirlpool? Smart fridges are an attack vector. And for a supply chain attack, the smart fridge or smart car does not need to be the final target. Any smartphone that connects to an infected IoT device could be used for further penetration of a target firm. This only heightens the need for everyone to take cyber risk seriously.

Ever Increasing Sophistication

All of the above underlines the increasing sophistication of potential attackers. With the resources and training of governments, and growing knowledge of weak points, it is no longer enough to simply follow normal safety procedures. Organizations will need to start proactively looking for and defending against potential cyber attacks, not merely hoping that existing procedures are sufficient. This will impose further costs on firms, and also raises the risk that governments will impose more stringent requirements for any vendor which deals with government organizations.

Frameworks for Cybersecurity

*What can be done about this growing risk? The obvious answer lies in cyber security frameworks such as **NIST CSF** that can deliver powerful risk management across the organization. There are a variety of options available:*

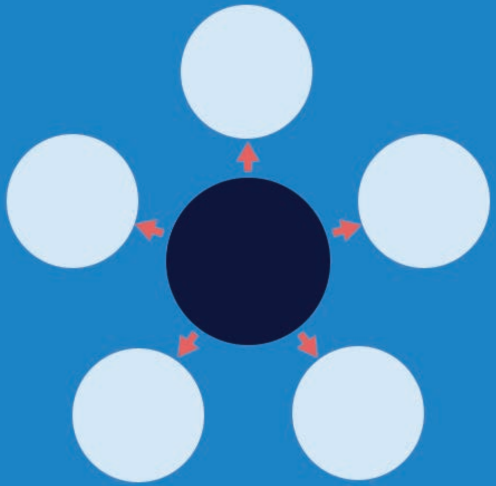


SABSA stands for the Sherwood Applied Business Security Architecture. SABSA is an open standard, generic, and vendor neutral, with a framework that is scalable and can be used by any industry or organization. The main feature of the SABSA model is deriving everything from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited.

As a framework, SABSA is best equipped to tell you what is important in cybersecurity terms, making it a strong tool for justifying aspects of a security architecture.

NIST CSF is an abbreviation that refers to the National Institute of Standards and Technology Cyber Security Framework, which was developed in 2014 in the US. The framework provides a high-level taxonomy of cybersecurity outcomes as well as a methodology to assess and manage them. As of May 2017, all US federal agencies are required to implement it – though the attack on SolarWinds has demonstrated the weakness in this approach.

NIST covers 5 areas of cybersecurity: Identify, Protect, Detect, Respond, and Recover, which have further subcategories and tiers of action, making it a strong framework for prioritising actions to take



COBIT 2019 is the latest comprehensive business focused framework created by ISACA that provides a Governance and Management framework for Enterprise level IT. While not solely focused on risk and security, COBIT 2019 takes risk management seriously. As well as the two dedicated processes in the Governance (Evaluate, Direct, and Monitor) and Management (Align, Plan and Organize) domains, which represent Ensure Risk Optimization and Manage Risk respectively, risk management is embedded throughout the COBIT 2019 framework.

As a governance framework, COBIT is best used in conjunction with a security framework like NIST, enabling architects to have oversight of their security implementations.

OTHER OPTIONS...

There are a plethora of other risk management frameworks, standards and processes. There is COSO for ERM, the RIMS Risk Maturity Model (RMM), Project Risk Management (in Prince2 or PMBOK), and the ISO 31000 family to name a few.
Having named all these alternative security frameworks, you might expect some kind of ranking or recommendation as to which is best, but ultimately all of these frameworks are in use because they are all useful in different situations. The most important action to take: pick a security framework and stick to it, across the enterprise, if you haven't already.

Responding to an Attack

Let's assume that you are already a secure organization, with a fully supported risk management framework and an in-depth cyber security policy. As the Sunburst hack has shown, even with all of this, you can still be vulnerable. How do you respond when an attack gets through?

Identify Every Breach at Once

Security Architecture and the associated frameworks are not necessarily about threat management or the direct implementation of protective measures, but rather the oversight and control of your cyber security. They enable organizations to fully leverage frameworks across the enterprise, but some aspects of cyber security are not the domain of architects.

However, one key ability that an EA tool like iServer could provide is the ability to track every instance of a breach or infiltration once it has been identified. For example, if an attack occurs against a specific SQL server, it is trivial to then identify every other area of the business that may be affected and remediate the issue all at once, instead of chasing down vulnerabilities one by one.

Have an IT Risk Management Toolbox

An IT risk management toolbox provides a set of templates and techniques that can be used by risk managers and auditors to assess, define and control material IT-related risks in an organization. Tools and techniques should support the risk management process. Example categories of tools and techniques may include: 1) Risk management policies and procedures; 2) Asset identification and risk assessment templates; 3) Reporting; 4) Document management and relational database systems.

Define Business Specific Risk Scenarios Applicable for Your Organization

As with the previous suggestion, this is a common tool of security frameworks. Risk scenarios lay out the potential dangers to an organization, without first needing to be targeted by an actual malicious actor. Risk scenarios can be likened to the missing link, bridging the gap between the intangible and unrealistic, to the tangible reality of risks to the organization, and ultimately the ability of the business to create and sustain value over the long term. When executives and stakeholders can clearly (and simply) see the scenarios that could unfold, should probable risks materialize, and their potential direct impact to the enterprise, support and decision making becomes more efficient and effective. And with that comes risk optimization.

Conclusion

The continued growth of cyber attacks, particularly those led by national governments, will pose heavy risks to enterprises. Defense has always been in a losing battle with attack, and this is certain to get worse as the resources available to hackers increase, and more vectors of attack are exposed. Every IT professional, or even every business professional, has a duty to think about security, not just risk professionals or architects.

Orbus Software
Floor 4, 60 Buckingham Palace Road, SW1W 0RR
+44 (0) 20 3824 2907
enquiries@orbussoftware.com
www.orbussoftware.com