Third-Party Cybersecurity Matters

June 2017
Fortium Partners, Cybersecurity Team

Conventional wisdom suggests employee access is the weakest link in enterprise cyber security. However, Soha System's (now an Akamai company) reported, in recent years, 63 percent of breaches can be traced to third-party vendors. Third-party cybersecurity matters now more than it ever has before.

The Internet, along with Internet of things (IoT) is so entrenched in the business world that nearly all things are connected to the outside world. This connectivity already includes: Point-of-sale devices, door access control, video surveillance, voice-over-IP telephone systems, A/V systems, HVAC, elevators, office machines and other appliance-type equipment that communicate via the Internet or the company's internal computing environment, and it is growing daily.

IT systems contractors operate similar to construction trade organizations. These companies are frequently called value-added resellers or VARs. IT systems contractors can be distinguished from professional service organizations with full-stack IT engineering, meaning technical expertise at all 7 layers of a computing network.

HVAC and Cash Registers

Two high profile reported examples include: 1) Target's, HVAC vendor being hacked and unwittingly provided the "trusted" access to Target's network. The Target systems were notably in complete compliance with security standards at the time of the hack. So, Target's security was compromised most likely because the HVAC vendor had no customer-facing cybersecurity protocol on paper or in mind, when that field organization installed the new equipment. 2) Wendy's fast food restaurant chain suffered a breach when attackers used login credentials of a third-party point-of-sale system to gain access to more than 1,000 franchise restaurants, including customers' credit card information. Other recent high-profile breaches resulting from third-party compromises include large discount chain stores, pharmacies and medical centers. These breaches are still being investigated and many may be traced back to third party vendor systems. Today's reality is that third-party connectivity is the weakest link in cybersecurity.

Despite an enterprise's best efforts to obtain compliance for its own systems, it is impossible to succeed in maintaining a secure posture without coordinating with third-party vendors, frequently referred to in contracts as "trusted associates". By coordinating, we are not proposing that such vendors comply with some security standard for back-office IT security. That, we believe, is misguided.

Instead, we recommend addressing your vendors' customer-facing security practices…those practices used when a vendor is touching your systems or your data. These customer-facing practices directly impact, negatively or positively, your company's vulnerability to cyberattacks and thus your security. Your vendor's field staff may be doing you a disservice when they are installing or servicing your organization's systems, and how could you possibly know one way or the other?

A vendor’s IT organization can be in complete compliance with a valid cybersecurity standard and still not be a safe vendor for you. At the same time, a vendor whose IT department is not in compliance can have a well-thought-out, customer-facing cybersecurity protocol that raises the standard of their services for your systems and data to a level that is highly secure.

IT systems contractors provide solutions for building access control, video surveillance, HVAC, voice-over-IP telephone systems, audiovisual, point of sale, and other systems.

So, which is better for you and your organization, a valid and mature customer-facing, security protocol and no back-office compliance or poor customer-facing security and full compliance? Although a vendor having both would be nice, we believe you agree that that best choice is for your vendors to have a mature, customer-facing security protocol. This is especially true for your IT systems contractors and their field organizations. The security of your organization can be dramatically improved by simply encouraging your IT systems contractors to define their customer-facing security protocols and then to share them with you.

Beyond Assessments and Compliance

Fortium Partners recommends organizations begin by requiring each of its third-party vendors to prepare a statement of the cybersecurity controls each vendor uses when touching, accessing, maintaining, or repairing your systems and data. We believe this is far more productive than conducting an assessment or compliance of back office systems with standards. Fortium will prepare a two-to-three page summary document that identifies 40 or more cybersecurity controls specific to each vendor, plus a written assurance that the vendor’s management promises to use “reasonable efforts” to meet the stated service level. This statement can be modified from time to time, as new customers and new products are acquired.

If you have any doubt about where to start this process, you can know that the most impactfully positive results and strongest ROI, meaning least expense and in less time, will result from starting with your IT systems contractors. These vendors provide systems such as door access control, video surveillance, audiovisual, voice-over-IP telephone, HVAC and others mentioned above.

Finally, Fortium recommends that the third-party vendor, pay for whatever assistance they need to prepare what Fortium offers a Cybersecurity Service Level Statement, a.k.a. Cybersecurity Protocol. Combine this with a request that the vendor and Fortium attest that the vendor’s staff is trained to conform to its own Cybersecurity Statement and that management will use “reasonable efforts” to assure the Protocol is implemented with each service or installation.

Most third-party vendors are happy to learn you have a solution for them that is also valuable to all their customers. With Fortium, they will be able to assure all their customers, and especially your organization, that security is a top priority.

As technology executives providing CIO services to dozens and dozens of organizations, Fortium consistently finds that systems contractors have excellent skills with the application software they provide and most of them have solid skills installing the physical layer. However, with very few exceptions, these same contractors have limited or no expertise with the network layers that exist between the application layer and the physical layer. Fortium studies indicate the greatest vulnerabilities often stem from vulnerabilities found in these middle layers of the network architecture, and, of course, above the secure sockets shell (SSH) protocol when cloud-based systems are involved. These are the two most prominent sources of attack surfaces used by hackers.

Know Your Third-Party Vendors

Fortium recommends that end user organization create and maintain a current register of each vendor, including their contact information and the systems and a description of the data they can access. A regular review of all third-parties should be part of any security review.

You can expect each of your vendors to prepare and provide a service-level statement of their cyber security practices, and how those practices apply to you (the customer). Simply contact them directly, or have a third-party such as Fortium do this for you, and ask that each prepare a a statement of their cybersecurity practices. In addition, you might give them an assist and recommend an independent party to mentor them through the process of preparing their service-level statement. They just might need that assistance. They might even thank you for your interest and support, as it could prove to be a service differentiator for other clients as well. Helping your vendors deliver security as part of the solution they typically offer is one of the great win-wins available today.

Brad Wheeler, Area Managing Partners, Fortium Partners, brad.wheeler@fortiumpartners.com

About: Fortium Partners is a national firm comprised of 70 technology executives having held positions as CIO or CISO or CTO in such nationally prominent organizations as Harvard University, Google, Apple, Symantec, Jacobs Engineering, Acer, and many others. Fortium's partners typically enter into multiple, simultaneous engagements on a fractional (part-time) or interim engagements. Fortium's Cybersecurity Practice engages with clients directly or in a support role as a member of a Fortium's Client Engagement Team.