A Standardized Online Business Relationship Schema

Summary: *Security has moved beyond perimeter and defense-in-depth, and is expanding its reach into the cloud. New models must be developed to adequately describe the dynamic, diverse requirements of a distributed business ecosystem. A light-weight, scalable, standardized, business-relationship schema would support this new mode of Ecosystem Security.*

Internet security vendors are typically focused on protecting companies, employees, and their customers from becoming the victims of malicious attacks. With a variety of solutions, we defend against attacks directed at a company and identify risks within the organization. Typically, they combine to enhance perimeter defenses, protecting against all manner of attack, from malicious payloads to Business Email Compromise (BEC) and phishing. The goal is to protect the final mile of an attack from succeeding.

Shifting the focus from enterprise protection, some solutions even enable companies to protect their partners and customers from impersonation attacks. These technologies help to ensure that, when receiving an email from a protected company, a receiver is able to verify it as legitimate. The goal is to ensure email sent by an authorized sender can be verified and, by extension, deceptions can be detected and treated accordingly (e.g. rejected, or quarantined for additional analysis).

Despite the measurable protections these solutions provide, it is clear that a focus on the organization itself is overly narrow. Protecting a company against specific attacks and known attack vectors is necessary, but doesn't leverage all of the signals available to detect (and act) earlier in the communication process. Now that these approaches have proven their value at enterprise scale, it's time to leverage them more broadly to Internet scale.

Enter the Ecosystem Security model. This approach builds upon the entity-centric view and expands it to all entities who rely on each other to operate in a secure and trustworthy environment. The goal is to understand that there are security issues that can only be addressed as a community. Essentially, we recognize there are security gaps that can't be filled by a company on its own, or hiring a vendor to lock them down for you. With that in mind, the Ecosystem Security mission is to tackle Internet security issues with a mix of technical standards along with industry and regulatory policies. Accomplishing such a lofty goal requires dedication to long-term vision of the future, with a team of experienced collaborators driving toward sustainable solutions for all stakeholders.

When extending security beyond the perimeter of a single organization, the complexities compound significantly. A lot of the experience earned when securing the enterprise, including a strong perimeter and defense-in-depth monitoring, doesn't directly apply to the process of securing an entire ecosystem. The traditional "castle with a moat" model, especially when taken to extremes, no longer applies. Especially given how often one must lower the drawbridge.

For example, some IT security practitioners would like to treat all external communication coming into the enterprise as "untrusted". Many will add an [EXTERNAL] label to subject lines of inbound email, delineating the divide between "us" and "them." Presumably this enables the employee to be more aware when interacting with potentially suspicious email. While that approach has its place to raise awareness when a message originates outside the company, what happens when the label is ignored? Unfortunately, habituation to this warning happens when employees regularly communicate with trusted external suppliers.

Consider, then, if the paradigm was shifted from “inside=good” and “outside=suspicious” to something more nuanced. Given that business requires communicating with vendors and partners, who are presumably trusted to some degree, there must be a way to codify these relationships. The simplistic form of this is whitelisting “trusted” external organizations. This often takes the form of identifying organizations, usually by domain or IP address, then placing them on lists that allow them to bypass security defenses. Unfortunately, a simple “pass” through specified defenses puts all whitelisted communications into the same category of trust.

The introduction and rapid adoption of ASP and SAAS models, exacerbated by the acceleration in shared cloud computing infrastructure, further blurs the line between “good/bad”, “friend/foe”, and just plain “unknown”. At this point, even if a partner is deemed to be trustworthy, it can be nearly impossible to separate their traffic from that of other users sharing the same multi-tenant infrastructure. And while many issues can be addressed with various forms of authentication credentials within exposed APIs, email communication remains the most abused vector for BEC and phishing attacks leading to infiltration and data breaches.

The foundational question remains: With whom is a company communicating and for what purpose? Only once that is answered, can truly scalable and effective security models be applied to a complex, dynamic, and highly-distributed set of business relationships.

A path toward answering this question may be found by exploring the success of the eduPerson schema developed to support the needs of higher education. While not a solution in-and-of itself, the schema was able to bridge a significant divide in the representation of entities (in this case, students) across highly disparate applications without requiring centralized control. Once developed to a sufficient degree of detail, the assertions could be leveraged by various interoperable IAM systems. Through the process of identifying, codifying, and standardizing key assertions, eduPerson became essential for enabling effective IAM for over 20 million students each year.

In a similar fashion, and following a similar development process, we propose the creation of a standardized set of core terms asserting business operations and authorized external relationships. Once developed, security organizations would be able to tailor some security signals to specific use cases at scale. For example, if a company publishes a set of attributes (e.g. within DNS) defining their business related to a set of domains and/or IPs, security vendors can leverage the information when evaluating signals for suspicious activity.

About Proofpoint:

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 100, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. No one protects people, the data they create, and the digital channels they use more effectively than Proofpoint. More information is available at www.proofpoint.com.