AMERICAN CITY&COUNTY

Cybersecurity questions every local government should ask its vendors

Written by Mike Duffy
20th July 2021

Recently, I took my kids to a Cubs game at Chicago's Wrigley Field. In the front of our section there was a fan dressed in the opposing team's gear. I'll call him "Steve." Multiple times each inning, Steve would stand, turn to the section and tauntingly gesture like an umpire when events of the game went against the Cubs. Seeing an opportunity for a dad life lesson, I leaned over to the kids and shared some deep wisdom: "This guy's asking for it!" As a crowd wave crested upon us, Cubs' legend Ryne Sandberg (or a fan wearing his jersey) charged down the aisle and fired a half-full beer cup into the back of Steve's head, point blank. He never saw it coming.

When it comes to cybersecurity, the public sector can learn a lot from Steve. He was too exposed and surrounded by too many motivated threats. So are too many public sector agencies.

Imagine the cup was a brick, Ryan Sandberg stole Steve's minivan keys and the entire stadium knew that Steve's family could pay a million dollars in bitcoin to ensure Steve was able to operate the morning carpool. This is the world we live in.

The COVID pandemic was a catalyst for governments to embrace technology and modernize public services to provide a better digital experience for both citizens and staff. However, this rapid digital transformation also introduced considerably more endpoints and, as a result, a much greater attack surface for hackers to exploit. This opportunity, combined with the potential for a major payout, has given hackers more incentive than ever to launch attacks against these lucrative government targets.

Considering the odds, governments and public sector entities who haven't yet fallen victim to a cyberattack shouldn't take it as a sign of security—but as evidence that no one has tried hard enough yet.

You can't secure what you can't see

Local governments have a lot of stuff to manage. You're likely wrangling myriad on-premise systems for dozens of departments. With disparate systems, each has its own attack surface and security monitoring program, or lack thereof.

Alternatively, integrated systems have fewer points of potential failure. Fewer applications, servers and network connections reduces the complexity, the risk and the maintenance that

impact system performance. Using the hosted services of innovators in the private sector is a simple way to reduce your complexity.

In the City and County of San Francisco, for instance, the Office of the Treasurer and Tax Collector has integrated its two dozen departments to a single system that powers web payments for the entire city-county. You don't have to be San Francisco to take this tech-forward approach. The City of Lawrence, Ind., is accelerating information security for their 50,000 customers and consolidating payment systems for both their online and in-person channels.

No matter the specific priority, it is the responsibility of governments to identify and implement solutions that provides citizens with the secure and resilient payment processes they expect.

Where you may not have a clear picture—or any picture—is the security of the third-party systems you partner with to handle personal identifying information (PII) for public-facing services like water payments, online permitting, grant applications, or tax billing and deduction applications. Legacy vendors have a massive cost to bring old systems up to current security standards, and you want to be sure that these non-revenue-generating expenses are being incurred on your behalf.

Understanding your vendors' approach to security

Asking specific questions of your vendor can help shed light on how your systems and your constituents will be protected. Here are a few things you should look out for to ensure your partner takes your defense seriously.

1. **What information do I *need* to show this customer to complete this service or payment?**

Having any PII readily available can put a target on you as a service provider. Before even thinking about your vendor, make sure you're collecting and displaying the minimum amount of PII possible. For example, if you are allowing someone to pay for their parking ticket online, you should only show the amount owed, license plate number, and date of issuance. Additional information on the individual like the car owner's name isn't needed to make the payment, and it should not be readily available for anyone to see.

2. **What security technologies do you have in place for event and threat detection?**

There are several open source and commercially available tools that modern software companies use for security. Your vendor's answer should be succinct and specific.

3. **A common scam is one where customers receive a fake link to an official looking website that tricks them into sharing personal information. How do you protect against this?**

Bad actors can mirror the look and feel of your website if they are determined to collect data from your users. If your users are accustomed to clicking out to a third-party site on an unfamiliar domain, it makes them more susceptible to these "fake" websites. Make sure your vendor allows you to keep your payment activity on your official domain, it's the best way to instill confidence and train your users not to trust unofficial third-party sites.

4. **If users complete payment on the official .gov domain, are you using iFrames to process payments? Who is responsible for the Payment Card Industry Data Security Standard (PCI) compliance? Who is responsible for securing the space between the official domain and embedded domain?**

Keeping customers on your official website and domain inspires confidence in the security of the transaction. However, iFrames aren't a great solution. The PCI Security Standards Council warned in 2017 that iFrames "are susceptible to compromise by a determined attacker." Since then, hacking payment pages and tampering with the embedded iFrame has become an extremely popular attack. The use of an iFrame also means you are still on the hook for PCI compliance, since you host the system which embeds the iFrame. Additionally, you're responsible for securing and monitoring the void between the official website and the embedded website, since the vendor can't see traffic that doesn't reach it.

Getting answers (that may terrify you)

So, how do you know your systems are secure? These questions are a great way to start getting answers. How do your vendors proactively monitor security-related incidents? Will they provide you the same view they have into attempted attacks on your system? If they don't know or don't have clear answers, it's time to find a new partner that uses a security-first approach.

Source: https://www.americancityandcounty.com/2021/07/20/cybersecurity-questions-every-local-government-should-ask-its-vendors/