In our attempt to be transparent and share information with all stakeholders; we sometimes inadvertently share sensitive information that could compromise the cyber security posture of the organization.

Sensitive organization information that could compromise your cyber security posture

Shivaji Sengupta

The open government data movement began fully maturing in early 2009, at a time when government(s) and society began to truly realize the beneficial value of government data; and open standards were taking root as drivers of innovation. The thrust of this movement was to identify all valuable Government data sets, and to require agencies to make them available to the public, at no cost, and in open-standard formats that ordinary citizens and enterprises could easily access and leverage.

These key principles were enshrined in the Data.gov initiative, established in May 2009, by, then-Federal Chief Information Officer (CIO) of the United States. Ten years later, Data.gov still serves to provide public access to high value, machine readable datasets generated by the Executive Branch of the Federal Government, creating the first publicly available repository for federal, state, local, and tribal government information.

Another milestone for open government data was the Digital Accountability and Transparency Act of 2014 (the DATA Act), which established a legislative mandate that government data be made freely available in standardized, open formats.

As part of the above initiatives some organizations and government agencies have published important information technology and privacy related documents and data on public facing websites that could be used by bad actors, adversaries and cyber criminals using this kind of data to launch ransomware attacks like the one on the City of Baltimore in May 2019, Lake City, FL in June 2019, Jackson County, GA in March 2019 and many others including Lynn, MA, Cartersville, GA and others.

In our attempt to be transparent and share information with all stakeholders; we sometimes inadvertently share sensitive information that could compromise the cyber security posture of the organization.

As government continues its efforts to make information available to the public there are many clear cases where information should be held private and/or redacted. Information which could violate the security of an individual, a business, or even the nation, should be closely guarded.

Here are internal data points / information that should not be shared on public facing websites:

Usernames: Usernames and passwords are separate entities but they do go hand-in-hand. When we talk about figuring out new authentication options. We need to give equal time to the username as we do the password. It's important to remember that when we just have a

username, it is easier than we realize to match that name with a password, simply because users still have trouble with password management.

Company Roster(s): Attackers are often after confidential data, such as credit card data, customer names, email addresses, and social security numbers. The reason for this is they can use a combination of name, email, username etc to entice an unsuspecting user to click on a malicious link etc. The company roster is an easy place to start where you can generally figure out the persons email ID through their name and the standard company email format. This is the first step for our adversaries.

IP Addresses: This "address" is your IP address, or Internet Protocol address. Your digital devices work much the same way as your physical address your device needs an address in order to send information to another device. It seems harmless, but attackers can actually launch attacks against you (or in some cases disguised as you) if they know your IP address. There are many reasons why cybercriminals might want your IP address, ranging from just messing with you to future larger-scale, targeted malicious attacks. Three of the main reasons they're on the hunt for IP addresses are to do to the following:

a) Download illegal content under your IP address' identity - They can download pirated movies, music, and videos—which would get you in trouble with your ISP—even pornography or content that threatens national security
b) Hunt down your location for larger-scale attacks: When given an IP address, an attacker can use geolocation technology to identify what region, city, or state you're in. They use this to decide if your area is a worthy target for future attacks.
c) Directly attack your network: Criminals can not only use your IP address for larger-scale attacks, but also to directly target your network and launch a variety of assaults. One of the most popular is a DDoS attack (distributed denial-of-service). This type of cyberattack occurs when bad guys use previously infected machines to generate a high volume of requests to flood the targeted system or server.

Computer Naming Schema: One existing risks is of computer naming schema on our a network. Usually you can easily identify host roles and running services just by their computer name (using tools such as nslookup). It is recommended to use less obvious computer names to improve the difficulty for an attacker to identify machine roles on the network. The

benefit is an attacker will need to spend (significant) more effort in determining the layout of your network and to identify the most valuable targets for a penetration attempt.

Database Names: Databases contains mission critical data of an organization, which makes it an obvious target by for hackers and bad actors. Usually a database server is not hosted in a less secure demilitarized zone; hence the bad actor has to by-pass the web layer to access the database. A database is a widely and continuously accessible component, which makes it more vulnerable and susceptible to attacks. Database security requirements touch all networking layers and need careful design. Database names should not be public information as it makes it much easier to identify and subsequently use tactics like Packet sniffing, Query string manipulation, SQL Injection, Database DoS to cause damage to the digital asset or service continuity.

Identifying Service providers / IT infrastructure service providers: Supply chain attacks have been in the news recently as vulnerable IT service providers are much more likely to create an entry point into a business network. Symantec reported that supply chain attack incidents went up by 78% in 2018, and a recent report by endpoint security firm Carbon Black estimates that 50% of all attacks are now targeting supply chains. The entry point could be a basic barrage of phishing emails that could target the service provider's employee accounts. From there the attacker may install malicious software and conduct a multitude of activity across various service provider clients. Businesses should already be screening the security policies and practices of vendors before going into business with them. There is a need to continually monitor their security stance and cyber readiness over the lifetime of the relationship.

Data Supply Chain: While we all focus on core IT, servers, applications etc we tend to forget that all a lot of the data is generated through automation, sensors and IOT devices. There is an increasing focus on securing our data supply chain to ensure accurate data is generated and transmitted to all business support systems, applications and other data collecting systems. This threat is usually of lower importance as adversaries are typically remote and do not have physical access to the data generation assets cause issues. However, it is prudent to keep the design, location and other information about these sensors / IOT devices protected.

Commercial Off the Shelf (COTS) Software: One of the biggest threats to any organization is

the vulnerabilities of COTS software where typically an organization has limited visibility into the code base or has the resources to do vulnerability assessments on all its software. The best practice is to ensure all COTS applications are updated as far as security patches are concerned and even update software which are no longer supported by the vendor. To minimize the risk to the organization it is prudent not to publicize the use of COTS software and tools that are used in the organization to ensure adversaries may not be able to readily use vulnerabilities that are within the software products.

Contributors

Shivaji Sengupta is a management, solutions development and delivery entrepreneur who has over 25 years of experience providing solutions to government and commercial customers. Mr. Sengupta is a member of the Homeland Security Committee and the Small Business Committee at Armed Forces Communications and Electronics Association (AFCEA). Mr. Sengupta is also an Adjunct Professor for Cyber Security at Delaware State University. He has designed and is teaching the Applied Cyber Security Course at DSU. Mr. Sengupta's company NXTKey Corporation provides cyber security solutions to key federal government agencies supporting them in maintaining their cyber defensive posture.

www.nxtkey.com