Talk Nerdy To Me

1

January 2020

5 Security Resolutions to Prevent a Ransomare Attack in 2020

Proactively consider tools to detect anomalous behavior, automatically remidiate, and segment threats

Over the past two years, ransomware attacks have increased in frequency and severity. In 2019 alone, the attacks have crippled manufacturing businesses, brought hospitals to a halt, and even put lives at risk. It's no wonder that many organizations are putting ransomware prevention and response planning at the top of their priorities list for 2020. And those that aren't probably should consider what more they can do to better prepare their organizations against these types of attacks.

The time to put measures in place is **not** after an attack has already taken place. Here are five things organizations should consider as part of their security resolutions in 2020:

Basic Cybersecurity Hygiene: Cybersecurity hygiene can mean a lot of different things, but a good place for companies to start is by making sure they have strong vulnerability management practices in place and that their devices have the latest security patches. They can also make sure they are taking basic security precautions that are often also important for regulatory compliance, like running up-to-date antivirus software or restricting access to systems that can't be made compliant.

Penetration Testing: Companies that already have much of the basic hygiene in place can take the additional step of engaging pen testers to further ensure that anything Internet-facing in their organization is protected. By finding what means or mechanisms attackers could hack or brute-force an attack to gain access to applications or internal systems by bypassing other protections such as firewalls, security leaders can fix those areas before bad actors find them.

Board Discussions: Cybersecurity is increasingly becoming a board of directors-level issue. That's because an attack can have a significant impact on a company's revenue, brand, reputation, and ongoing operations. However, it's worth having a specific board-level conversation about ransomware to ensure they understand the specific risks it could pose to the business, and that there is budget made available to prevent or limit the damage of an attack. That discussion will prove critical if the company wants to implement added protections, such as improved cyber hygiene, or put in place automated reactive technologies to limit the spread of an attack. If the CIO or CISO is not already regularly having these conversations about cybersecurity or ransomware in particular, that's definitely a good place to start for 2020.

Tailored Training: There is one vulnerability that has proven effective again and again as an entry point for attack: people. You can buy all the latest and greatest cybersecurity technology, but if you aren't training your employees in basic cybersecurity or how to respond during an attack, then you're leaving yourself vulnerable. Training to prevent ransomware starts by teaching employees to recognize phishing attacks and what to do if they suspect one.

Limit the Scope of an Attack: Ransomware resolutions should include not only preventing an attack but also taking steps to minimize the damage of a successful one. That starts with having tools in place that can identify the behavior patterns and heuristics of an attack and begin to automatically isolate and remediate those systems when indicators are flagged. It also means embracing tools such as network segmentation that can prevent the lateral movement of an attack across the network.

Source: Darkreading.com

Top Data Breaches of 2019

If you do a quick search on the Have I Been Pwned website, you will get a list of how many times your personally identifiable information (PII) has been found online. The free service aggregates data breaches and is managed by Troy Hunt, a known expert cybersecurity developer. It also helps establish if your credentials, such as IP addresses, emails, passwords, usernames, geographic locations, name and social media profiles have been found in data breaches. At the end of September, there were 5,183 breaches, exposing 7.9 billion records. Compared to September of 2018, the total number of breaches was up 33.3 percent and the total number of records exposed more than doubled, up 112 percent. Here are some of the top data breaches of 2019.

ElasticSearch Server Breach – 108 Million Records
In January 2019, ZDnet reported that an online casino group leaked information on more than 108 million bets, including details about customers' personal information, deposits and withdrawals. The data leaked from an ElasticSearch server that was left exposed online without a password. ElasticSearch is a portable, high-grade search engine that companies install to improve their web apps' data indexing and search capabilities. Justin Paine, found the user data included a lot of sensitive information, such as real names, home addresses, phone numbers, email addresses, birth dates, site usernames, account balances, IP addresses, browser and OS details, last login information and a list of played games.

Canva Data Breach – 139 Million Records
In May 2019, Security Magazine reported that Canva, a graphic-design tool website, suffered a data breach that affected 139 million users. The data exposed included customer usernames, real names, email addresses, passwords and city and country information. In addition, of the total 139 million users, 78 million users had a Gmail address associated with their Canva account. According to ZDnet, the hacker responsible for this breach has put up for sale on the dark web the data of 932 million users, which they stole from 44 companies from all over the world.

Third-Party Facebook App Data Exposure – 540 Million Records
In April 2019, UpGuard security researchers revealed that two third-party developed Facebook app datasets were exposed to the public internet. One database originated from a Mexico-based media company, and weighed in at 146 gigabytes with more than 540 million records detailing comments, likes, reactions, account names, Facebook IDs and more. The other third-party app, "At the Pool," was exposed to the public internet via an Amazon S3 bucket. This database backup contained username IDs, friends, likes, music, movies, books, photos, events, groups, check-ins, interests, passwords and more.

Dream Market Breach – 620 Million Records
In February, The Register reported that some 617 million online account details stolen from 16 hacked websites were on sale on the dark web. The following account databases were being sold on Dream Market: Dubsmash (162 million), MyFitnessPal (151 million), MyHeritage (92 million), ShareThis (41 million), HauteLook (28 million), Animoto (25 million), EyeEm (22 million), 8fit (20 million), Whitepages (18 million), Fotolog (16 million), 500px (15 million), Armor Games (11 million), BookMate (8 million), CoffeeMeetsBagel (6 million), Artsy (1 million), and DataCamp (700,000).

"Collection #1" Data Breach – 773 Million Records
In January, Troy Hunt announced he had found a set of email addresses and passwords totaling 2,692,818,238 rows, made up of many different individual data breaches from thousands of different sources. In total, there were 1,160,253,228 unique combinations of email addresses and passwords. Unique email addresses totaled 772,904,991. Unique passwords totaled 21,222,975. Multiple people reached out to Hunt and directed him to the collection of files on the cloud service MEGA, which contained over 12,000 separate files and more than 87GB of data.

Verifications.io Data Breach – 808 Million Records
In April, Diachenko and Vinny Troia, reported that they had found a publicly accessible MondoDB database that contained 150 gigabytes of detailed marketing data. The databased was owned by the email validation firm Verifications.io and was taken offline the same day Diachenko reached out to the company. The database contained four separate collections of data, totaling 808,539,939 records.

First American Data Breach – 885 Million Records
In July, a data leak at First American Financial Corp., the largest real estate title insurance company in the U.S., exposed transaction records of 885 million individuals. According to Brian Krebs, American journalist and investigative reporter, First American leaked hundreds of millions of documents related to mortgage deals going back to 2003.

TrueDialog Data Breach – More Than 1 Billion Records
Based in Austin, Texas USA, TrueDialog creates SMS solutions for large and small businesses and currently works with over 990 cell phone operators and reaches more than 5 billion subscribers around the world. The TrueDialog database, hosted by Microsoft Azure and run on the Oracle Marketing Cloud in the USA, included 604 GB of data. This included nearly 1 billion entries of highly sensitive data.

Social Media Profiles Data Leak – 4 Billion Records
In October, Diachenko and Troia found a trove of data exposed and easily accessible to the public on an unsecured server, which contained 4 terabytes of PII, or about 4 billion records. A total count of unique people across all data sets reached more than 1.2 billion people, making this one of the largest data leaks from a single source organization in history.

A few other data breaches reported throughout the year are: Capital One, State Farm, Biometric Records, DoorDash, Choice Hotels, European Hotel Group, and Sprint.

Source: Security Magazine

BEFORE THE BREACH

HACKERS ARE HERE!

NEW SKILLS FOR A NEW FIGHT

- 1 in 5 businesses will suffer a cyber breach
- this year
- 81% of all breaches happen to small/medium sized businesses
- 66% of companies do NOT test their backups
- 60% of companies that lose their data will go out of business within 6 months
- 92% of malware is delivered via email
- 97% of breaches could have been prevented with today's technology

Want to learn more about how to protect your business?

Stay tuned for our next lunch and learn in March!

RUTH'S U.S. PRIME CHRIS® STEAK HOUSE

www.preferreditgroup.com/beforethebreach

talk nerdy to me

PREFERRED IT EMPLOYEE SPOTLIGHT

Meet Gabbi Rex! Gabbi has been with Preferred IT Group for 9 years! If you've called into our office, chances are that you've spoken with her. She is responsible for the day to day coordination of work getting accomplished by our amazing technicians and engineers. She is a third of our company's leadership team and helps to make the decisions that move our company forward.

Gabbi also heads up all of the Technology Alignments with our managed customers every quarter. She is starting to work her way into sales and marketing as well.

Gabbi is a wife and soon to be mom of two boys. She has a great dane named Isabelle. She is the resident coffee addict in the office and is always listening to the Hamilton soundtrack while she works. If you walk into her office you'll know she's a huge Harry Potter nerd and a fan of old Marilyn and Audrey movies.

Gabbi is a valuable member of our team and we'd be lost without her!

Head-Turning Ransomware Attacks to Hit City Governments in 2019

Hackers know vulnerable systems when they see them, and they also know this: Many government systems are decades old, running Windows 7 and even Windows XP.

In July, the Georgia court system was hit with a ransomware attack, resulting in at least part of its digital information systems being taken offline. Back in 2018, Atlanta was also hit with ransomware that caused millions of dollars in loses.

Riviera Beach, Florida paid in excess of $600,000 to restore the municipality's systems from a ransomware campaign. A police department employee opened a malicious email attachment which ultimately disabled the city's online systems including email, a water utility pumping station, some phones, and the ability to accept credit card payments. A similar attack also happened in Lake City, Florida.

The city of Baltimore, Maryland was hit with an attack that locked down it's servers and left the city's government without email, telecommunications, and disrupted real-estate transactions and bill payments. The city lost about $18 million in damages.

Similar attacks also happened last year to West Haven, Connecticut, Johannesburg, South Africa, Greenville, North Carolina, and the state of Louisiana.

Source: darkreading.com

PITG CHRISTMAS PARTY

Preferred IT Group had a blast at our Christmas party this year! We were treated to dinner at Baker Street and as always, the food was fantastic!

After dinner, most of us ended up at the Double Dragon for a round of gaming! What else would a bunch of IT nerds do to party the night away ;)

preferred IT group

CONTACT US

Fort Wayne	260.440.7377
Warsaw	574.306.4288
Columbia City	260.213.4266
Indianapolis	317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.