Moving to Proactive Cybersecurity

By Anthony Scott Thompson

Introduction

Currently, cybersecurity is prescribed as a series of reactive events and “forensics” actions. Cybersecurity is currently, for the most part, handled through education, firewalls and “breach response”. By the time the latter happens, isn’t it too late? Wouldn’t it be better if we could stop these breaches from happening in the first place?

Moving to proactive cybersecurity is not just a good idea, it will be required. This paper explores where most vulnerabilities lie and where you have your largest exposure. We will also look at what is coming and how to prepare for it.

What is Broken?

What is being done now for cybersecurity does not work. From Equifax to Anthem to Sony to the DNC, breaches are becoming increasingly costly. We are beginning to see where breaches may start to destroy business or at the very least tarnish reputations eroding trust. In this section, we will explore the roots of the problems.

Networks Built on Trust Everything

The Internet was initially created from a series of government funded networks. At that time, everyone on the network trusted everyone else. Focus was put on being able to inspect the network to figure out and solve networking issues. The assumption was, if you were on the network, you were probably a trustworthy person. This was a closed community of scholars with no concerns over security.

Before the final restrictions on carrying public traffic ended in 1995, the Communications Assistance for Law Enforcement Act (CALEA) was passed. Because of the distributed nature of the Internet, to be compliant with this law, providers of telecommunications services and, by proxy, Internet equipment providers, are required by law to have surveillance capabilities. Because of this, small ISPs and large cloud providers that provide backbone infrastructure to the Internet, have the ability to record data from any source, anywhere including other countries.

The combination of overt trust and laws requiring the ability to record data have led to an Internet that is fundamentally not secure. Moreover, because Internet protocols were not designed for public use but for diagnosing problems, those diagnostic features can be exploited directly in the network. Companies jumping on using the same networking protocols inside their internal networks and connecting all computers and devices to the Internet have created the cybersecurity fiasco we see today.

The power, utility and economic incentives the Internet provides from email to the economy of scale provided by Cloud Computing offsets the concern. The belief is the reward is much greater than the risk but is that really a true? According to the coveted Cost of Data Breach Study, the average cost of a single data breach in 2017 was $7.35 million, up 5% from 2016. In a small to midsize company, a single breach could be catastrophic. Even for large companies, multiple attacks will pile up the costs. If there is more valuable or damning data like in the Sony breach, those costs to brand will pile up for years later.

The Power of The Web

Let’s face it, the Internet is incredibly powerful. Any information you want is at your fingertips. It is not possible to put that genie back in the bottle - it is a resource every employee expects to have when they sit down to start any job. How many employees do you think your company can attract if you ban or even restrict Internet Access? You would be hard pressed to develop a general workforce if you took that away.

That power has also extended to systems through Web Services. These allow the creation of programs that can use data from multiple resources with relative ease. Applications are no longer being installed but sent to us over the Internet being managed and maintained by a single company in The Cloud. This paradigm, like the web browser, is also too powerful to contain.

With that power, comes great risk. Because the underpinnings of the Internet were built on trust a pandora's box of security problems exist. Reactive solutions, besides happening after the fact, simply do not address the real issue - the design of the protocols and equipment do not meet their new purpose of public and commercial use. Throw in a law that requires that anyone with an Internet router to be able to record data from anywhere and a huge security problem is created. Without fundamental change, information control is truly lost.

...But My Data is Encrypted!

All current standard encryption uses some form of short key or key(s) with well known algorithms. Some newer techniques will rotate keys but the new keys are typically transmitted

across the same communications channel as the data so key rotation is, in most cases, easy to capture and, in all cases, trivial to detect. So here is the problem with this technique: the key or keys are sitting on both sides of the communication. The simplest way to capture these keys is to get hired and gain trust. This could be a short term contract position hired as a subject matter expert - trust is immediate. Like the keys to your house or car, once they have them, they have access. If they are recording the data, they can now decrypt at will and, worst of all, you will never know it. Moreover, even if the keys are rotated, they are traveling across the same channel and will be intercepted or, if the perpetrator has installed remote access, they can simply lift the new keys and will know exactly when to do it.

What is more alarming is there are an increasing number of cryptographic attacks available allowing an attacker to calculate the keys or simply crack the encryption. What was discovered with the 2013 NSA leaks is encryption has been compromised for years mostly, as the foremost authority on encryption Bruce Schneier has put it, “through cheating”. Purpose built exploits have been (and likely still are) embedded in the encryption calculations to create “back doors”.

What is equally alarming is we’re also facing a looming Quantum Computing threat. In simple terms, this means there will be methods to decrypt current encryption directly. IBM, Google, Microsoft, Intel and others are spending heavily to unlock the power Quantum Computers. While still in research, Quantum Computers actually do exist and are not theoretical. It is concerning enough that the NSA is exploring new methods that will avoid the looming quantum threat.

The fact remains that whether it be simply “lifting” keys, “cheating” encryption algorithms or calculating the key from a supercomputer, your encryption is not safe from someone who is determined. Combine that with the relative ease with which data traveling across the Internet can be recorded and you need to start seriously questioning the actual security of your IP VPN and Cloud Services.

Shy of purchasing expensive, private lines to create an isolated WAN and rejecting all forms of Cloud Computing, your data is, simply put, not secure.

Why The Firewall Is Not the Perfect Solution and Never Will Be

Firewalls are intended to be a virtual stone wall between the Internet and your company's network. This sounds like a great idea and the metaphor of protecting the company from “Fire” is a powerful one. They are marketed, with great success, to keep the bad guys out. The issue is, what happens when someone or something inside the Firewall connects to the outside? Your firewall has a hard time discerning bad from good data without inspection of every packet. Deep inspection is not practical and, if data is encrypted, there is no way to really tell the bad from the good anyway.

An employee simply has to go to the wrong site clicking on the wrong link and suddenly outsiders have access to your corporate network along with everything connected to it. Software vulnerabilities can also allow a remote connection to be made from inside the Firewall. Either provides access to start hacking and cracking systems and data.

With the issues of hiring the bad guy, clicking on the wrong link or installing tainted software, there is no amount of AI, packet inspection or breach monitoring that is going to stop this. The fundamentals of the problems are simple and easy to exploit. In short, Firewalls, while an important tool to address some very obvious issues with IP networks, will never be able to adequately address connections from the inside without restrictions that hinder productivity. At this juncture, this reality is self evident.

Lurking in The Cloud

Cloud services have provided us with an economy of scale never seen before. Instead of having to manage email servers, you simply purchase email as a service from a company that takes care of the systems administration details for you. This allows companies to start up on tens of dollars a month for something that would have previously required a modest staff. In short, the cloud has freed entrepreneurs from the yoke of large IT budgets. At the same time, this is also starting to free existing, larger companies of those same costs. As with the web, it would seem that same proverbial genie can not go back in the bottle.

There is a huge issue with this approach though. As we discussed earlier, US law has required vendors of large, Internet specific network equipment to build in recording capabilities to capture data from anywhere on the Internet. If you know the IP and port, rerouting a copy of that data is trivial. More concerning, this does not have to be the federal government or even someone in this country. Anyone with an Internet router compliant with US law can do it.

What this means is our cloud services are completely exposed to recording. There are other means like Man in the Middle attacks that can be used to record data as well but the fact remains that our data can be easily recorded. There is no magic to doing this and more and more competitors and rogue agents have these capabilities.

Also, as discussed, the way encryption is handled currently, it is only a minor inconvenience for someone that is determined. Almost all cloud services use public key encryption which absolutely can be compromised by stealing the authentication cert and public key from the authenticating Certificate Authority (CA) or tricking the client into installing a fake cert spoofing the CA. These are not theoretical but real, practiced vulnerabilities. In the future, today's encryption may not even be an inconvenience. Just remember, what is recorded today can be

decrypted at any time in the future when computing power increases and Quantum Computers are a commodity product. If the information is useful for a long time, as many corporate documents and emails are, that is problematic.

Building Proactive Cyber Defense

So, how do you actually protect your data and still maintain the economy of scale created by Cloud Computing and Cloud Networks? The solution is to have proactive defense techniques. These remove access, increase encryption effectiveness and make data recording an order of magnitude more difficult. There are three main areas to consider with cyber defense:

1. Networks
2. Software/Hardware
3. People

If you can solve all three of those problems proactively, you start to remove vulnerabilities en masse.

Keep Moving to Protect Data In Motion

The US Department of Homeland Security (DHS) has identified Moving Target Defense as a technique that can protect both data in motion as well as data at rest. For recording data either via Man in the Middle or directly from an Internet router, the connection in the network needs to be static and never moving. When you change or move “the channel” the data resides on, you now have disabled the ability for current recording techniques to be employed.

Encryption That Cannot Be Hacked

Traditional encryption is susceptible to multiple attack vectors (e. g. sideways attacks) and, in the future, quantum computing. However, the ability to encrypt data in a way that cannot be breached has been around for over 100 years. Because of increases in network bandwidth and data storage, it has become possible to leverage these time tested techniques using an innovative approach. This works by having a never-ending stream of random data that is sourced from the real world, is not calculated and cannot be guessed. This is simple to derive from the noise in a sensor reading when it is read many decimal places to the right where it becomes a quickly changing, random number. The room you are sitting in right now will have a temperature reading that, if read with enough precision, becomes chaotic. This is what is referred to as a “state of entropy”. They are the only form of true randomness known and can be used to create encryption that cannot be solved by a computer or cheated creating rigged

algorithms. When this data is sent across a network, we refer to it as a Streaming Key or Streaming Key Encryption. This is derived from an encryption technique used by the military called a Vernam Cipher.

Solving For Data In Motion

Introspective Networks has developed and patented a solution that uses both Moving Target Defense (MTD) and Streaming Key Encryption (SKE) to protect data in motion like never before. This technique is called Streaming Transmision One-time-pad Protocol, or STOP. This technique hides the data in the network as well as encrypting data using the same technique for critically secret information.

The Right Place for the Firewall

Firewalls have been traditionally set at the edge of the network. Intuitively this seems like the right place - separate the Internet from the WAN from the LAN. While this seems intuitive, it has been proven to be largely ineffective. Also, the amount of processing power required to actually inspect packets, identify breaches and alert is prohibitively expensive. Simply blocking traffic is not enough; as we've explored, the connections are being established from inside the company network.

So, while the idea of a partition sounds great, where exactly is the best place to do this? The answer is right at the computer. Introspective Networks has developed a solution called a Partitioned Access Workstation (PAW) that completely separates the "public" from the "private". If you download something from your web browser, that ransomware will not have access to the "private" side. This includes data in motion as well as data at rest. When combined with STOP based network solutions, you have a complete, proactive cybersecurity solution.

Adding Machine Learning and Artificial Intelligence to Proactive Driven Security

Currently there is a scramble by Cybersecurity companies to use Machine Learning and Artificial Intelligence (ML/AI) to speed up both breach recognition and breach response. This is limited by latency, processing power and resiliency. If there is not enough processing to do deep packet inspection, there is certainly no power left for something like ML/AI. That said, ML/AI can be applied to increase your holistic cybersecurity program.

Currently there is an area of research called "the automation of knowledge work". This is fundamentally using Multi-Agent Systems to take over repetitive, although possibly complex,

tasks performed in a plant of some kind. We've seen this in manufacturing of complex systems like automobiles and will start to see this move towards critical infrastructure like power grids and telecommunications networks as well as the newly forming markets in autonomous aerial and automotive vehicles. This removes the possibility of people making critical errors or for nefarious individuals to infiltrate critical infrastructures. This automation increases security and resilience using ML/AI in way that requires a feasible amount of processing power.

By using ML/AI, we remove the human element that, in many cases, is too slow to respond. In other cases, humans can be persuaded through social engineering or just bad judgement to create cyber breaches. ML/AI can remove these threats to our most critical existing and forthcoming infrastructures.

Introspective Networks has also addressed this solution with a distributed ML/AI framework: Processing Units for Multi-Agent Systems, or PUMAS. This allows for single purpose distributed processing with zero-nines uptime and subsecond recovery from processing or network failures. When combined with STOP, you have a robust, zero nines, highly secure IoT infrastructure solution.

Conclusion

What the market is doing for cybersecurity is simply not working. Firewalls can not handle the inside threat, ML/AI is too resource hungry, and encryption is undermined as well as woefully inadequate. Lastly, as we move more and more of our data to IP networks and the Internet, we are working in a system that was never designed for security. The CALEA law has also created an Internet recording capability that can be exploited undetected from anywhere in the world.

With all this, it is time to take a fresh look at how cybersecurity is implemented. Proactive cybersecurity solutions, at all levels, disconnect risk factors almost completely. Whether it be IoT or your company office, with Introspective's solutions, the question of breaches is simply removed. The time for action is now - contact us to learn how to reduce your cybersecurity exposures proactively.

About the Author: Anthony Scott Thompson has been architecting, securing and developing global parallel and distributed systems for two decades. He has an advanced degree in Computer Science from the University of Colorado and has multiple granted patents to his name. He is the Founder of Introspective Power, Inc. dba Introspective Networks - a company dedicated to increasing network security and solving the most complex problems around IoT.

References:

1. https://www.internetsociety.org/internet/history-internet/brief-history-internet/
2. https://en.wikipedia.org/wiki/History_of_the_Internet#World_Wide_Web_and_introduction_of_browsers
3. https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance
4. https://en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act
5. http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption
6. https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html
7. https://www.dhs.gov/science-and-technology/csd-mtd
8. https://www.scrypt.com/blog/average-cost-data-breach-2017-3-62-million/
9. https://www.schneier.com/blog/archives/2015/08/nsa_plans_for_a.html