Human Error: The Downfall of Giants

“It’s our ignorance that allows for breaches in data. There is a proverb that drives this point home. He who ignores the time walks in darkness, and he who explores it is illumined by a great light. We must walk in the light of knowledge and shield customer credentials from prying eyes.”

Dirty Deeds Done Dirt Cheap

On average, Ransomware costs Hackers between $250 and $650. It’s hard to believe, but malicious software costs less than the a jalopy, and, this metaphorical second-hand car takes Ne'er-do-wells further than the corner-store. For their flyspeck investment, Cyber-criminals hijack data for millions of dollars! In fact bargain-bin saboteur software has become the norm.

For instance, Stampado sells on the Dark Web for $39. Far more shocking, some commonly used hacking software is free, Kali Linux is an open-sourced operating system that provides tools for isolating weaknesses in networks, it costs nothin'. Yet, Kali Linux, and other such Pen Testing distributions are doled out with good intentions, unlike Stampado.

All told, Stampado is no master of disguise. It’s easily detected and removed from networks. Stampado may not bring-in the clams, but a modified version of it, Philadelphia Ransomware, currently sells for $389. Philedalphia Ransomware is stealthy, yet budget conscious. Worst of all, this affordable tidbit of malicious software can’t be detected by most antivirus applications. It’s a digital sniper for would-be Hackers.

Frighteningly enough, Ransomware is constantly evolving. In fact, “developers have modified their software to offer complementary capabilities,” these modifications enable malicious-software-makers to provide a suite of malevolent utilities, known as Ransomware as a Service (RaaS), with no money-up-front.

“Ransomware 2.0,” as it was dubbed by a CISCOMag, is stealthier, sneakier and easier than run-of-the-mill virus 1.0 for scoundrels to unleash on your network.

If they give it away for free, how are malicious-software makers making money? Surprisingly, profit sharing is a popular business model in the shady world of Ransomware, but I guess that’s where the phrase “thick-as-thieves” originates, bandits share among themselves.

In this model, Hackers divide the profits, an 80/20 split in favor of the Cyber-criminal, with malware developers. This business model is referred to as or no-cost profit sharing.

Collectivivism among crooks aside, Ransomware 2.0 allows Hackers to “select the targeted file extensions [or] directories, set a ransom, convert currency [between nations] and input a Bitcoin address for payment, [all] within a simple Graphical User Interface that completely eliminates the need for any coding or command line skills."

The moral: Ransomware is easy to come-by, a cinch for nogoodniks to set into action (there's no coding needed) and often enough bankable.

At its' core, Ransomware is a malignant code designed to prevent access to files, on a compromised system, until financial demands are met. These business crushing applications "leverage public key infrastructure (PKI) [and] siege autonomous offline encryption. [Worst of all these programs] are self-propagating." Further dishearteningly, Ransomware is just a drop in the sea of viruses that could infect your network.

But Placing all the blame on Ne'er-do-wells is downright dishonest, it's our ignorance that allows for these breaches in data. In fact, there is a proverb accredited Moses Ben Ezra, a Jewish poet, that drives this point home. Ben Ezra said that "he who ignores the time walks in darkness, and he who explores it is illumined by a great light."

All things considered, each and everyone of us must be a zelig: master our roles in the office while remaining abreast of best practices. If we disobey this adage and open the door to digital viruses, we neglect to defend company assets. These days, we must walk in the light of knowledge and shield customer credentials from prying eyes.

Small Mistakes Big Trouble

Decision Based Error

Not too long ago, Equifax's IT cadre passed an email along regarding a vulnerability in Apache Struts, software for developing web applications in Java. Their geek squad should've rectified the problem, but didn't. This inattentive work ethos allowed for 155 million sensitive files to fall into the hands of Hackers.

In total, decision-based human error "exposed the personal information of 145 million people in the United States and more than 10 million UK citizens" to ne'er-do-wells.

"This sort of error [occurs] when a User makes a faulty decision." As for the Equifax Team, IT failed to update Apache software and the company was fined $594,505.

No red flags were raised on that Spring day in 2017, although a costly bungle took place, an "oversight enabled a digital attacker to crack into Equifax's system in mid-May and maintain their access until the end of July."

Skill Based Error

It was a typical day in Strathmore, Australia. On this ordinary day, slapdash work allowed for publishing more than 300 student records on Southmore Secondary College's intranet. These files included student medical aliments, mental health maladies and prescribed medications, along with any learning or behavioral disorders that students may suffer; the kind of information that's sheilded by HIPAA.

Disquietingly, skill-based human error caused Strathmore Secondary College student records to remain on their intranet for about a day. The sum of the damage in unknown, students and parents had unfettered access to information that should only be seen by a doctor.

This sort of error "consists of slips and lapses, small mistakes that occur [while] performing familiar tasks and activities" in a slipshod manner.

No alarm bells sounded on that August day in 2018, although a colossal blunder took place, student files were left in the open for all to behold the secrets that they hold.

Password Based Error

It was a slow day when Veeam, a backup and data recovery company left a database wide open. A sloppy Tech Team neglected to password protect classified data: 200 gigabytes of customer records that included names, email and some IP addresses, the sort of thing you should never share with stranger on internet.

Password-based human error caused Veaam to expose a database to Hackers. This sort of error occurs when we use weak passwords or leave the password blank.

No siren rang out on that August day in 2018, although a flub took place, Veeam was forced to shutdown their server.

Bad Actors Get the Better of You

Remember this, upon opening the door to viruses, downloading and installing them, these crafty coded creeps can "use your machine's system connection to seek out all computers on the same network. and after, viruses endeavor to abuse all network-based vulnerabilities."

Email.

It goes without saying that email is the weakest link in this chain. In fact, "email accounted for over half of all malware infection attempts in 2020, making it the most common method of spreading [malicious software]."

I have a tale to tell, during 2018, the United States Department of Defense forwarded an unencrypted email with an attachment to the wrong distribution list. The email exposed personal information of approximately 21,500 Marines, sailors and civilians. It included “victims’ bank account numbers, truncated Social Security Numbers and emergency contact information.” It was a case of misdelivery.

This type of error “was the fifth most common cause of all cyber security breaches. With many [office personnel] relying on features such as auto-suggest in their email clients, it is easy for any User to accidentally send confidential information to the wrong person.” Hopefully, this cautionary anecdote demonstrates just how easy it is for haphazard fingers to destroy lives and industries.

Spreadsheets

Far worse, “Excel formulas, which cannot be blocked [via anti-virus software], [can conceal] malicious code: Outlook, FaceBook and Office 365 were the most popular brands spoofed in phishing emails.”

"The thing about Excel Formula macros is that unlike normal [scripts written in Visual Basic], you cannot disable the macro code." And so, it's wise to avoid downloading Excel sheets from less than trusthworthy sources.

Firmware

“Woefully, Firmware viruses aren’t that unusual, "80% of enterprises were victims of at least one firmware attack in the past two years.” Despite being ordinary, these attacks can be deadly for industries that work with sensitive information.

A VPNFilter, a particularly viscous firmware virus, installs malware onto the router. This in turn collects files and data as it’s compressed through network devices.

Not just does this wicked software sniff-out data from traffic, it installs additional malicious plug-ins that monitors network traffic to grab sensitive User information. In addition, this heinous software initiates packages to convert HTTPS web traffic into unencrypted HTTP, so that nogoogniks can extract your login credentials or account information.

Ransomware

And, Ransomware is often spread through phishing emails, emails that like a Catfish, pretend to be something they aren’t. They make-believe that they are important documents, but in reality, the attachments contain malicious software.

Crypto-ransomware, a variant of this malignant software that encrypts files with both AES and RSA, is disseminated via email and social media that uses web-based instant messaging applications.

Adding it Up

When we add it up, "human error accounts for 95% of cyber security breaches." Conversely, all but 5% of destructive data incursions and Ransomware installs are avoidable. Bad Actors will exploit vulnerabilities, it's an undeniable fact. But, it's up to us to, though diligence, protect assets.

You may have heard the spiel before, but we must continually update our knowledge base and walk in "a great light" as the proverb goes. Doing so protects the one thing on Earth more valuable than oil or gold, data. Knowing this, it's imperative to become an factotum (italics), mastering our role while fending off Hackers, for giants may fall through careless fingers.