Powered by GLESEC

CYBERSECURITY NEWS

Generated on 03/03/2020 by Sergio Heker

CUSTOM REPORT

3 Simple Steps to Keep Employees Current on Cybersecurity

03/02/2020 15:01

Source: pikrepro.com

John TeehanFollowMar 2 · 4 min read

Worried that your business might fall victim to a phishing scam, a malicious link, or ransomware? It's a reasonable fear given the rise of cyberattacks over the past decade. What's worse is that despite the best efforts of brilliant minds, the attacks keep coming and they're coming from ever-more-sophisticated sources.

That's why your employees are such an important part of your cybersecurity strategy. It doesn't matter how thorough your firewalls and monitoring software are, it means little if your employees haven't been trained to recognize threats when they appear.

If you want to protect your business from cyber threats, it's up to you to make sure your employees have the proper training. Here are a few ideas to get you well on your way to a secure business

information network.

Source: pikrepro.com

Starting with a clear set of policies should be the first step you take. If employees have guidelines to refer to and follow at the very beginning, you're more likely to be able to stop bad habits before they start. Ideally, it should be a major portion of any employee orientation and as part of an orientation packet.

Give them a copy of the policies in writing their first day on the job.

The first policy outlined for new employees should be your password policy. Include such requirements as using at least one number, one symbol, and one capital letter. You could even go so far as to require that the capital letter not be the first letter of the password, nor the number or symbol be the last. Encourage your employees to create passwords that break obvious expectations.

In addition, remind your employees to not write their password down and to change their password

every three to six months.

A simple password policy can go a long way in protecting your network. In the end, set policies give your employees the guidance they need to stay well within cybersecurity best-practices.

When new cyber threats rear their ugly heads, you need to get the word out to your employees sooner than later. Forewarned is forearmed, and if they come across the latest threat, they'll be less likely to be caught off guard.

The simplest, quickest way to inform employees of new threats is to send out a quick company-wide text notification or email. These messages or emails don't have to be particularly involved. A simple link to an article outlining the latest threats should be sufficient. The point is to bring as many people in your organization up to speed as possible without having to make it a day-long chore.

You don't necessarily have to do it yourself. An office manager or IT team member can be given the responsibility of sending out the company-wide messages. Assign them the responsibility of checking cybersecurity news every week or two and make sure that employees know as part of their initial orientation to always check emails from these employees.

Source: peakpx.com

Handouts at orientation and some emails or text messages here and there aren't enough by themselves. While they're both effective tips, you should take things a step further and establish a system of regularly scheduled training sessions to keep staff up to speed on the latest cybersecurity developments both inside and outside of the company. This will also impress upon your employees exactly how serious you take cybersecurity as a business practice.

These sessions don't have to be long. Every three months, a 30-minute to an hour-long session should be sufficient to cover a quick rundown on current cybersecurity policies and practices along with mention of the latest threats to be on the lookout for. That leaves plenty of time to cover an additional topic at each session such as the importance of software patching, what a phishing email looks like, or what to do when you suspect a cyberattack has occurred and you fear that business or customer data has been compromised.

When all is said and done, the greater the emphasis you place on caring about cybersecurity, the more your employees will pick up on that and do their part in keeping your business and customer data safe. And if all else fails, simply remind them that a serious enough data breach could result in

a significant enough loss of business that it may affect your ability to stay operative.

When it comes to cybersecurity, maintaining best practices is in everyone's best interest.

Master Email Security With SPF, DKIM, and DMARC Protocols

Earn customer trust by adopting these authentication protocols

medium.com

Protect Your Business With a Cybersecurity Assessment

You may think your network is secure but is it really?

medium.com

Thank you for reading. I'd love to share more with you via my **Weekly Word Roundup** newsletter sent to subscribers every Sunday. It will feature news, productivity tips, life hacks, and links to top stories making the rounds on the Internet. You can unsubscribe at any time.

Our Dangerous Reliance on Email Attachments And What To Do About It

03/01/2020 20:24 Alex PanagidesFollowMar 1 · 8 min read

Continuing to send email attachments is costly, dangerous, and unnecessary, given the readily available alternatives. It is time to tackle the root causes of our cybersecurity challenges rather than the symptoms.

Seemingly innocuous, email attachments are not. A design that dates back 50 years, inefficient from inception, has now become a destructive force diverting our precious resources as we continually tackle their collateral effects in collective resignation of a status quo that needn't be.

Around 306 billion emails are sent and received every day. In the corporate environment, about 25% of messages carry file attachments, or 76 billion messages [1]. These are big numbers. Among the biggest, when it comes to any communication today. It is past time to question this most common file sharing method, especially when considering the billions of dollars spent trying to mitigate problems that find their roots in this outdated technology. An astounding amount of resources (time, money, effort, and lost opportunity) are directed in an attempt to secure, govern, and manage the detritus of this archaic model of file exchange [2]. It is time to question, in particular, because for years, secure file links have stood as a readily available alternative.

The challenge of email attachments stems largely from two aspects of its architecture, namely, duplication (data sprawl) of content and the lack of security.

Email is data sprawl on an epic scale

The email attachment model of embedding a copy of a file into the message ensures that data will be duplicated. This duplicity grows exponentially when coupled with the common end-user behavior of copying (Cc, Bcc) and forwarding messages to others, even to those who will never open the embedded file. Taking available data, we can estimate the number of files each business worker sends and receives per year at 17,125 [7]. For lack of data, this calculation assumes that an email with an attachment carries on one file, which clearly underestimates the total number of files duplicated in email. In a previous article, we calculated that around 6,000 of these attachments are completely ignored. These numbers represent only the amount of files represented by the user's inbox, not accounting for copies in redundant servers and archival systems, which further multiply the quantity. Furthermore, those attachments that get read are often saved locally, thereby creating yet another copy in the recipient's device. Finally, and also not accounted for in these statistics, is the additional duplication resulting from the recipient's possession of multiple devices (e.g., laptop, mobile, etc.) — each which can receive its own copies. In an enterprise with one redundant email server and one email archive, we can comfortably assume that, at the minimum, each user represents more than 50,000 files per year.

File distribution by Email Attachments vs. Share Links. Attachments are copied every time email is stored & attachments are accessed. File links only copy when files are accessed. The scenario does not account for external systems copied (e.g., CRM) or copies created by forwarding the recipient's email system.

With email attachments representing, very conservatively, around 17,000 files per worker per year, we conclude that in a 1,000 person company a staggering 17 million file copies are created every year as a result of email's file-sharing methodology — or about 50 million file copies given email redundancy and archives, but not accounting for the copies used by recipients outside of the email message. Email is data sprawl on an epic scale.

Available statistics estimate, on average, around 55,000 file duplicates created per business user per year as a result of email attachments in a scenario of one redundant email server and one archive. The file copies accounted for by file Links only refer to downloads. There are no files in an email when sending a file link.

As a result of this explosive generation of duplicated content, most of it useless and all inefficient [3], our businesses, governments, schools and every organization that relies on email as their primary communication platform have to deal with an insurmountable challenge for information

security, governance, and infrastructure cost.

The data sprawl problem wouldn't be as bad if the files sent through email were encrypted or tracked. Unless the user takes extra encryption steps, email attachments are completely unsecure and provide no tracking of their whereabouts or who is looking at them. Each of those 17,000 files per user per year is readily accessible to whoever has a copy of the email, and that includes the hackers who breach the email system, backup servers, a misplaced device, PST file, etc. — whether in your organization or any organization you communicate with. Furthermore, given that email attachments provide no possibility of revocation after being sent when systems are breached, valuable corporate content sent years before is still there.

Like smoke from a diesel truck, information leakage, and its resulting liability, is the natural byproduct of our emails

The anonymity of attachments also facilitates their usage as a means of cyber-attack by bad actors. Commonly classified as the primary vector of attack, email and its attachments provide an ideal delivery mechanism by which to bypass company defenses and get malicious code executed on the user's device, well behind the company's firewalls [4].

The sheer volume, distribution, and lack of inherent security of email makes controlling our data an impossible task

Companies deploy millions of dollars in data loss prevention and data security solutions, from requiring multi-factor authentication, installing network border systems, to providing regular employee information security training [5]. In addition, regulations require responsible custodianship of data and penalize heavily for infraction [6]. But how can the CIO, even the savviest armed with the biggest budget, contain a fundamental architectural flaw inherent in the Internet's oldest and most widespread technology — an architecture that replicates, with viral efficiency, unprotected, untraceable copies of corporate content inside and outside of the organization, across multiple devices and systems!?

Actually, there is a solution, and there is a good chance you've used it. Partly in response to email's limitations, the rapid growth of cloud content storage platforms (e.g., Box, Microsoft OneDrive, Google Drive, Egnyte) provides a new model of file exchange. The cloud storage model does not send a copy of the file, rather a link to the file stored by the sender. This model is the direct opposite of the email attachment model. The benefits of the cloud storage model are multiple. The epic data sprawl caused by email attachments is reduced by more than 75%. Now files are only distributed to those who are interested. Eliminating the aforementioned 6,000 files per user per year that go unread. If we include the elimination of copies sent, but never read, on different devices, backups and redundant email systems within and outside of the organization, we can estimate a reduction of greater than 90% in file sprawl. With the drastic reduction in distributed

files, there is a concomitant reduction in network bandwidth and storage required to transmit and save unused files, plus an additional bonus reduction of 37% in file sizes from avoiding email's archaic file encoding mechanism [3]. Just accounting for attachments in users' mailboxes, available statistics attribute around 8Gb of files per business user per year — or around 7.8Tb for a 1,000 person company per year required by the email server, another 7.8Tb for any redundant servers, more for archival systems and more for attachments saved to local devices [1]. The use of cloud storage share links eliminates all the storage of attachments not viewed by recipients or copied to auxiliary email infrastructure.

The cost of rampant email data sprawl reflects not only in the number of files copied but also the bandwidth & storage required to transmit and store them all. Conservative estimates put a year's worth of email attachments for a 1,000 person company at 7.8TB or 20Tb when included email redundancy and archives.

With regards to security, cloud storage links offer significant benefits for the sender and recipient. For the sender, access to files can be controlled, requiring authentication, allowing only viewing (no download), and expiring even after delivery of the message. For the recipient, cloud links provide a safe preview of file content away from their local device, eliminating the dangers of malicious code execution. They also provide origination by pointing back with a secure URL to an authenticated cloud storage account that has an owner, complete with a detailed audit trail, and security controls over how the file got there. In the event of a malicious file deployed from a cloud storage account, internal IT can more easily contend with a single URL than a massively distributed email message. Finally, file delivery is encrypted end to end — of interest to both parties.

Impact of Email Attachments — there is little to celebrate in email's attachment file-sharing model

Like the oft-cited definition of insanity, businesses continue to dedicate significant time, money, and energy into problems originating from insurmountable challenges either directly caused or exacerbated by email. As the news cycle of email caused breaches proves to us on a daily basis, these efforts are of little avail. Until organizations recognize and resolve the root cause, they will continue their Sisyphean task, forever looking for and spending on the next technological miracle bandaid — be it Artificial Intelligence, Machine Learning, Social Graph, or another buzzword.

AI forecast: 'Disruption, then productivity' | Data Driven Investor

There is growing concern about all the white-collar jobs that will disappear with the spread of machine learning and...

www.datadriveninvestor.com

The reality is we are up against the fundamental architectural flaws of technology created decades ago and still in ubiquitous use today. These fundamental flaws have long been recognized. The seminal Internet Mail 2000 proposal posted by cryptologist and email technologist, Daniel J. Bernstein, outlined a new architecture whereby email would no longer be an analog to the postal service, i.e., where content is sent to the recipients, rather the recipients retrieve the content stored by the sender — a far more efficient design, simultaneously resolving email's problems of spam, bounces, content proliferation, and false origination. However, redesigning the Internet's most widespread communication infrastructure is a challenge. But we have entered a new moment, a moment where cloud content storage has become commonplace in the business world. With secure storage links, we correct the aforementioned flaws, bringing to fruition the known solution. Investments in user adoption training, increase in email client features for generating file links and services, like MXHero, that automate the creation of file links are far less costly than the perpetual, ineffective, and expensive game of whack-a-mole in common practice by organizations globally.

The reality is we are up against the fundamental architectural flaws of a technology created decades ago and still in ubiquitous use today.

Collectively we have a problem that is costing ourselves, businesses, and society billions and billions of dollars. We know the solution. For most organizations, cloud storage is readily accessible. It is time to prioritize and make it happen, namely, replace email attachments with shared links. We have so much more important things to do with our resources than to be trying to patch the collateral effects of a long-obsolete technology. Let's develop vaccines, solve global warming, educate our young. So please, for you, for me, for our world, no more email attachments.

When duplication is a good thing ;)

Sources

1. Radicati
2. CyberCrime Magazine
3. Cisco
4. Wikipedia
5. Gartner
6. SecurityToday
7. Methodology & Calculations (spreadsheet download)