On June 28, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, VMware, Fortinet, and Google products.
CIS Security Advisories

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN
30 June 2023

In The News This Week

Russian Cybersecurity Executive Arrested for Alleged Role in 2012 Megahacks

Nikita Kislitsin, formerly the head of network security for one of Russia's top cybersecurity firms, was arrested last week in Kazakhstan in response to 10-year-old hacking charges from the U.S. Department of Justice. Experts say Kislitsin's prosecution could soon put the Kazakhstan government in a sticky diplomatic position, as the Kremlin is already signalling that it intends to block his extradition to the United States. Kislitsin is accused of hacking into the now-defunct social networking site Formspring in 2012 and conspiring with another Russian man convicted of stealing tens of millions of usernames and passwords from LinkedIn and Dropbox that same year. In March 2020, the DOJ unsealed two criminal hacking indictments against Kislitsin, who was then head of security at Group-IB, a cybersecurity company that was founded in Russia in 2003 and operated there for more than a decade before relocating to Singapore. Prosecutors in Northern California indicted Kislitsin in 2014 for his alleged role in stealing account data from Formspring. Kislitsin also was indicted in Nevada in 2013, but the Nevada indictment does not name his alleged victim(s) in that case.... Read the rest of the story by Brian Krebs here: KrebsOnSecurity

High school changes every student's password to 'Ch@ngeme!'

After a cybersecurity audit mistakenly reset everyone's password, a high school changed every student's password to "Ch@ngeme!" giving every student the chance to hack into any other student's account, according to emails obtained by TechCrunch. Last week, Oak Park and River Forest (OPRF) High School in Illinois told parents that during a cybersecurity audit, "due to an unexpected vendor error, the system reset every student's password, preventing students from being able to log in to their Google account." "To fix this, we have reset your child's password to Ch@ngeme! so that they can once again access their Google account. This password change will take place beginning at 4 p.m. today," the school, which has around 3,000 students, wrote in an email dated June 22. "We strongly suggest that your child update this password to their own unique password as soon as possible." Needless to say, giving everyone the same password is not how an organization should force a password reset. The usual procedure is to force log out every user, and then prompt them to change their password the next time they try to log in. Manning Peterson, the mother of an OPRF student, replied that "this is terribly insecure, and you have just invited every single students [sic] accounts to get hacked."...
Read the full story by Joe Lorenzo Franceschi-Bicchierai here: TechCrunch

Pilot data of American Airlines and Southwest stolen in data breach

Personal information of 5,745 pilots of American Airlines and 3,009 pilots from Southwest Airlines has been leaked due to the incident. A cybersecurity incident at a third-party vendor has impacted the personal information of pilots of at least two US airlines, including American Airlines and Southwest Airlines. Personal information, including name and social security number, driver's license number, passport number, date of birth, Airman Certificate number, and other government-issued identification numbers were compromised, according to breach notifications from the airlines. On May 3, both airlines were informed that their third-party vendor, pilotcredentials.com, had experienced a cybersecurity incident involving some files within its systems. An unauthorized actor accessed the third-party vendor's systems on or around April 30 and obtained certain files provided by some pilot and cadet applicants during their hiring process, the airlines said in their notifications....
Read the rest of the article here: CSO

Siemens Energy confirms data breach after MOVEit data-theft attack

Siemens Energy has confirmed that data was stolen during the recent Clop ransomware data-theft attacks using a zero-day vulnerability in the MOVEit Transfer platform. Siemens Energy is a Munich-based energy technology company with a global presence, employing 91,000 people and having an annual revenue of $35 billion. It designs, develops, and manufactures a wide range of industrial products, including industrial control systems (ICS), state-of-the-art power, heat generation units, renewable energy systems, on and off-site energy delivery systems, and flexible power transmission solutions. **The company also provides a wide range of cybersecurity consulting services for the oil and gas industry, including incident response plans, vulnerability assessment, and patch management. Tuesday, Clop listed Siemens Energy on their data leak site, indicating that data was stolen during a breach on the company. As part of Clop's extortion strategy, they first begin listing a company's name on their data leak site to apply pressure, followed by the eventual leaking of data. While no data has been leaked at this time, a Siemens Energy spokesperson confirmed that they were breached in the recent Clop data-theft attacks utilizing a MOVEit Transfer zero-day vulnerability**...
Read the full article by Bill Toulas here: Bleeping Computer

Data Encryption, why is it needed?

I had many conversations in the past about what to encrypt, where to encrypt, and why to encrypt. There are various schools of thought around all three of these areas and for the layman, it can be very confusing. Today I want to share an article posted on TechCentral by Altron Systems Integration that touches on some of the what and the why. Granted that the article is written by a vendor that promotes their own solution, I felt that it gives a fair overview of the subject for those not traversing in the cybersecurity space.

Data encryption a vital cog in cybersecurity

Data has become one of the most valuable commodities. As a result, cybercrime has become a highly lucrative industry for modern criminals and a significant threat to businesses. Yesterday's tools such as firewalls, intrusion prevention and antivirus software are no longer good enough to prevent cyberattacks – particularly in a world of distributed workforces that has seen traditional business perimeters dissolve.
No entity is safe. From the smallest company to the largest enterprise, barely a day goes by without news of another breach, meaning that companies need new solutions to protect themselves and their most valuable assets.
Many forward-thinking businesses are turning to encryption, or the process of converting data into an unreadable form to prevent unauthorised access. When combined with other security measures, encryption dramatically reduces the risk of security threats.
Via encryption, data is transformed into a different form or code called ciphertext, which can only be accessed by those with the decryption key or password. The key consists of mathematical values and enables the data to be restored to its original form. Naturally, the strength of the encryption is enhanced by using a complex cryptographic key, which leads to more 'heavy duty' encryption.

Many benefits

Data encryption offers several advantages, protecting businesses that handle large volumes of data from security breaches that can damage their finances and reputation.
Encryption ensures data is protected in all states – while in motion and at rest. Business owners can also have peace of mind that their data remains secure and confidential, regardless of its sensitivity. While firewalls offer a level of protection against unauthorised access, they cannot prevent successful breaches if hackers manage to get through perimeter security measures.
However, if the data is encrypted, it becomes extremely challenging for hackers to decipher and also greatly reduces the chances of successful brute force attacks.
Because many industries are subject to stringent data protection regulations, encryption helps businesses remain compliant. Not only does encryption safeguard sensitive information by implementing encryption measures, but companies can also demonstrate their commitment to protecting data privacy and can avoid costly penalties associated with non-compliance.

Fostering trust

In an era where data breaches and cyberattacks are commonplace, customer trust is paramount. By implementing robust data encryption, businesses can assure customers that their personal and sensitive information is secure. This fosters trust and confidence in the company's ability to handle data responsibly, strengthens customer relationships and protects the company's reputation.
It's also important to remember that data encryption is not limited to customer data protection. It also plays a vital role in safeguarding trade secrets and proprietary information. Encryption prevents unauthorised access and helps preserve the integrity and confidentiality of valuable assets, providing a competitive advantage for businesses.

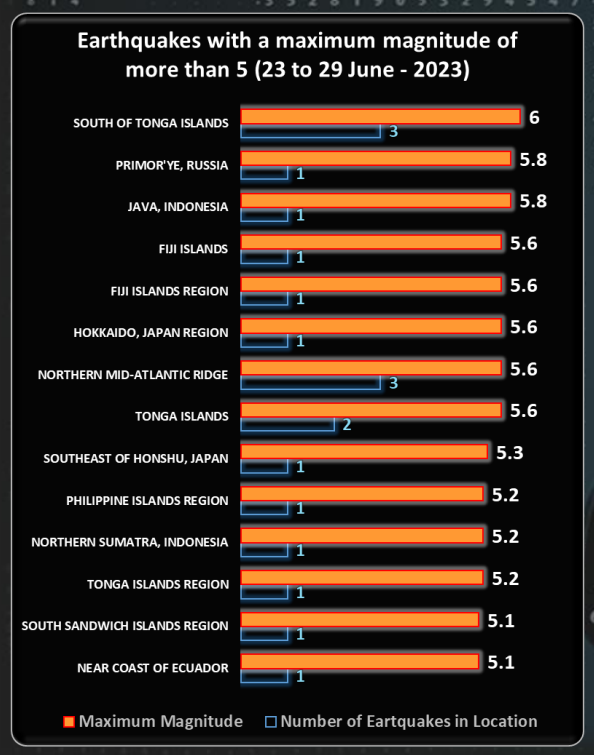
Uncompromising security

In today's remote work environment, data flows through numerous devices, making it crucial for businesses to ensure uncompromising data security. Companies face the challenge of limited control over how employees share and access data, and with potential security threats existing across personal devices, encryption plays a critical role in safeguarding data from unauthorised access. By using encryption, businesses can guarantee that data remains obscured and secure across any device.
Data manipulation and tampering are also a worry for businesses. Encryption not only protects against data tampering, but can help users identify any unsanctioned modifications, helping businesses maintain the integrity of their data.
Many industries operate under stringent regulations that enforce data privacy. For example, the healthcare industry adheres to HIPAA regulations governing the storage of sensitive patient data. Additionally, there are various data protection regulations such as Popia and GDPR, among others. Non-compliance with these regulations can result in hefty penalties for organisations, and encryption helps businesses to meet regulatory requirements and ensure compliance.

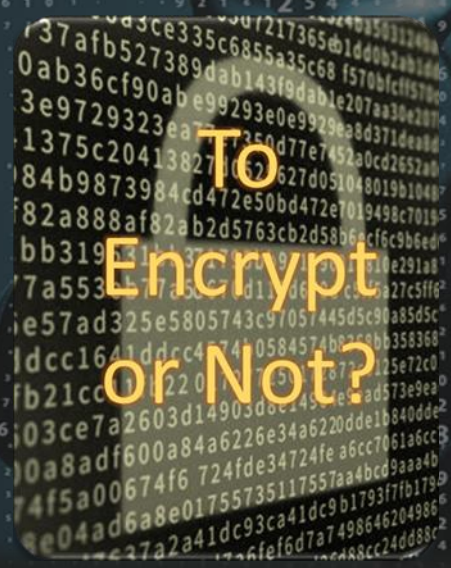
Keeping IP safe

Theft and manipulation of intellectual property (IP) pose significant risks in today's landscape, where cyber espionage is not as unusual as one might think. Safeguarding patents, copyrights, trademarks and trade secrets is of utmost importance. Data encryption plays a key role in preventing the unauthorised use or reproduction of copyrighted material, protecting valuable IP.
Data breaches have raised concerns among customers regarding the security and privacy of their personal information. As a responsible business that values its customers, prioritising security best practices is essential. By assuring customers that their business adheres to specific encryption standards to uphold data privacy, businesses can gain a competitive advantage and foster trust.
Implementing data encryption across the business is crucial for organisations that want to protect their data. Encryption safeguards data integrity, helps meet regulatory compliance requirements, protects intellectual property and enhances consumer trust. By leveraging these technologies, businesses can mitigate risks, maintain a strong security posture and instil confidence in their customers.

Resources: TechCentral



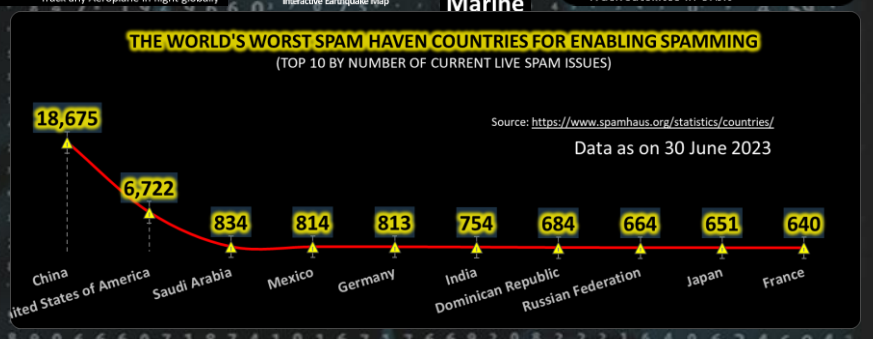
For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud



Other Interesting News and Cyber Security bits:

- BlackBerry Is Betting Its Comeback On Cyber Security
- Mockingjay – A New Injection Technique to Bypass Endpoint Detection and Response (EDR)
- Ensuring home network security: Essential tips to safeguard your digital world
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
IRIS Interactive Earthquake Map
Marine Traffic
SatelliteXplorer Track satellites in orbit



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com