NEWS D.A.D.

100% COVERAGE OF EACH & EVERY RELEVANT NEWS

SOURCES

PIB » The Hindu » Live Mint » HT » TOI
RBI » ET » Indian Express » PRS Blog and more…..

14 leading sources for **CURRENT AFFAIRS** covered on **Daily basis.**

“Every News counts and we make sure that you don't miss any relevant News.”

CRACKACADEMY

Index

Top White House cyber aide says recent Iran hack on water system is call to tighten cybersecurity . . . 2

Unseemly turn: The Hindu Editorial on Raj Bhavan’s relations in Kerala . . . 5

Why ransomware attacks on Indian IT firms are a cause for concern? . . . 7

Unjust and unwise: The Hindu Editorial on counter-insurgency operations in J&K . . . 10

TOP WHITE HOUSE CYBER AIDE SAYS RECENT IRAN HACK ON WATER SYSTEM IS CALL TO TIGHTEN CYBERSECURITY

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

To enjoy additional benefits

CONNECT WITH US

December 09, 2023 09:56 am | Updated 09:56 am IST

COMMents

SHARE

READ LATER

FILE PHOTO: Miniatures of people with computers are seen in front of binary codes and words 'Cyber attack' in this illustration taken July 19, 2023. REUTERS/Dado Ruvic/Illustration/File Photo/File Photo | Photo Credit: Dado Ruvic

A top White House national security official said recent cyber attacks by Iranian hackers on U.S. water authorities — as well as a separate spate of ransomware attacks on the health care industry — should be seen as a call to action by utilities and industry to tighten cybersecurity.

Deputy national security adviser Anne Neuberger said in an interview on Friday that recent attacks on multiple American organisations by the Iranian hacker group “Cyber Av3ngers" were “unsophisticated” and had “minimal impact” on operations. But the attacks, Neuberger said, offered a fresh warning that American companies and operators of critical infrastructure “are facing persistent and capable cyber attacks from hostile countries and criminals” that are not going away.

“Some pretty basic practices would have made a big difference there,” said Neuberger, who serves as a top adviser to President Joe Biden on cyber and emerging technology issues. “We need to be locking our digital doors. There are significant criminal threats, as well as capable countries — but particularly criminal threats — that are costing our economy a lot.”

The hackers, who U.S. and Israeli officials said are tied to Tehran's Islamic Revolutionary Guard Corps, breached multiple organisations in several states including a small municipal water authority in the western Pennsylvania town of Aliquippa. The hackers said they were specifically targeting organisations that used programmable logic controllers made by the Israeli company Unitronics, commonly used by water and water treatment utilities.

(For top technology news of the day, subscribe to our tech newsletter Today’s Cache)

Matthew Mottes, the chairman of the Municipal Water Authority of Aliquippa, which discovered it had been hacked on Nov 25, said that federal officials had told him the same group also breached four other utilities and an aquarium.

The Aliquippa hack prompted workers to temporarily halt pumping in a remote station that regulates water pressure for two nearby towns, leading crews to switch to manual operation.

The hacks, which authorities said began on Nov. 22, come as already fraught tensions between the U.S. and Iran have been heightened by the two-month-old Israel-Hamas war. The White House said that Tehran has supported Houthi rebels in Yemen who have carried out attacks on commercial vessels and have threatened U.S. warships in the Red Sea.

Iran is the chief sponsor of both Hamas, the militant group which controls Gaza, as well as the Houthi rebels in Yemen.

The U.S. has said they have uncovered no information that Iran was directly involved in Hamas' Oct. 7 attack on Israel that triggered the massive retaliatory operation by Israeli Defense Forces in Gaza. But the Biden administration is increasingly voicing concern about Iran attempting to broaden the Israeli-Hamas conflict through proxy groups and publicly warned Tehran about the Houthi rebels' attacks.

“They’re the ones with their finger on the trigger,” White House national security adviser Jake Sullivan told reporters earlier this week. “But that gun — the weapons here are being supplied by Iran. And Iran, we believe, is the ultimate party responsible for this.”

Neuberger declined to comment on whether the recent cyber attack by the Iranian hacker group could portend more hacks by Tehran on U.S. infrastructure and companies. Still, she said the moment underscored the need to step up cybersecurity efforts.

The Iranian “Cyber Av3ngers” attack came after a federal appeals court decision in October prompted the EPA to rescind a rule that would have obliged U.S public water systems to include cybersecurity testing in their regular federally mandated audits. The rollback was triggered by a federal appeals court decision in a case brought by Missouri, Arkansas and Iowa, and joined by a water utility trade group.

Neuberger said that measures spelled out in the scrapped rule to beef up cybersecurity for water systems could have "identified vulnerabilities that were targeted in recent weeks.”

The administration, earlier this year, unveiled a wide-ranging cybersecurity plan that called for bolstering protections on critical sectors and making software companies legally liable when their products don’t meet basic standards.

Neuberger also noted recent criminal ransomware attacks that have devastated health care systems, arguing those attacks spotlight the need for government and industry to take steps to tighten cyber security.

A recent attack targeting Ardent Health Services prompted the health care chain that operates 30 hospitals in six states to divert patients from some of its emergency rooms to other hospitals while postponing certain elective procedures. Ardent said it was forced to take its network offline after the Nov 23 cyberattack.

A recent global study by the cybersecurity firm Sophos found nearly two-thirds of health care organizations were hit by ransomware attacks in the year ending in March, double the rate from two years earlier but dipping slightly from 2022.

“The president’s made it a priority. We’re pushing out actionable information. We’re pushing out advice,” Neuberger said. “And we really need the partnership of state and local governments and of companies who are operating critical services to take and implement that advice quickly.”

COMMents

SHARE

technology (general) / cyber crime

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Source : www.thehindu.com Date : 2023-12-19

UNSEEMLY TURN: THE HINDU EDITORIAL ON RAJ BHAVAN’S RELATIONS IN KERALA

Relevant for: Security Related Matters | Topic: Role of External State & Non-state actors in creating challenges to internal security incl. Terrorism & illegal Migration

December 19, 2023 12:15 am | Updated 12:15 am IST

The conflict between the Governor and the Left Democratic Front government in Kerala has turned unseemly. Raj Bhavan’s relations with regimes other than those run by the Bharatiya Janata Party have been quite testy in recent years, and the problem is quite acute in Kerala. The issue arises from sharp political and ideological differences, as appointees in Raj Bhavan have made it a point to use their position as chancellor of universities as well as their constitutional role in granting assent to Bills to cause annoyance to elected governments. In a sign of rising acrimony, differences over appointments to the Senate of the Kerala University have snowballed into frequent protests. While student activists accuse the Chancellor, Governor Arif Mohammed Khan, of appointing right-wing sympathisers to the Senate, he has been complaining about political interference in the universities. In the latest incident, the University of Calicut saw dramatic scenes as activists of the Students’ Federation of India (SFI) put up posters against the Governor-Chancellor. The Governor has accused Chief Minister Pinarayi Vijayan and the State police of being behind the poster campaign against him. Some days ago, SFI activists blocked Mr. Khan’s car, resulting in some arrests.

Recent court judgments have underscored that elected regimes should not be undermined by unelected Governors. Such verdicts have drawn public attention to the partisan role played by Governors to stymie governance in States not run by the ruling party at the Centre. In a recent ruling, the Supreme Court of India set aside a reappointment given to a vice-chancellor in Kannur University on the ground that there was unwarranted interference by the government. Given that chancellors are expected to act independently, there is much scope for a clash with the government. However, responding to such situations through organised protests is not advisable. Chief Ministers should instruct their supporters to avoid street protests that turn belligerent. One way to resolve the issue is by legislation either removing Governors as chancellors or transferring the chancellor’s powers to any other authority. However, Bills containing such changes are not likely to get the Governors’ assent. This does make legal redress difficult for those aggrieved by what they deem to be arbitrary use of the chancellor’s powers. It may be time to think of a long-term solution in the form of a statutory prohibition on Governors being chancellors of State universities. The M.M. Punchhi Commission on Centre-State relations had recommended ending the practice of burdening Governors with the role of university chancellor.

SHARE

Governor / Kerala / university / politics / education / judiciary (system of justice) / Bharatiya Janata Party

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Source : www.thehindu.com Date : 2023-12-25

WHY RANSOMWARE ATTACKS ON INDIAN IT FIRMS ARE A CAUSE FOR CONCERN?

Relevant for: Science & Technology | Topic: Science and Technology- developments and their applications and effects in everyday life

December 25, 2023 08:30 am | Updated 10:47 am IST

On 20 December, IT services provider HCL Technologies, in its quarterly report, shared that it was hit by a ransomware incident within a restricted cloud environment. Following the attack, the company stated there was no “observable” impact on the overall HCL Tech network. However, news of the attack affected the company’s perception of the stock market, leading to a decline in its share prices.

HCL Tech is an Indian information technology company providing solutions in the digital realm, including end-to-end digital offerings, cloud-based solutions, and software.

The company is one of the top software solution providers in India.

On 20th December, the company, in its quarterly earnings report, sharedthat it was hit by a ransomware incident in an isolated cloud environment.

The company, however, did not disclose specific details of the attack.

HCL Tech further stated that cybersecurity and data protection are top priorities.

A detailed investigation, in consultation with relevant stakeholders, was launched to assess the root cause.

Ransomware is extortion software designed to lock or encrypt a device or data on a system and then demand a ransom for its release.

The attacks follow a simple plan wherein attackers gain access to a device or protected data in the cloud.

Depending on the nature of the ransomware, it will then lock or encrypt devices, data stored in the cloud, or the entire internal network of an organisation.

Attackers usually leave behind a message with instructions on the ransom amount, mode of transfer, or instructions on how to contact them for further guidance.

Indian organisations are increasingly targeted by ransomware attacks.

A 2023 study conducted by Sophos, a cybersecurity company, showed that 73% of organisations reported being victims of ransomware attacks, up from 57% the previous year.

Of these, 77% of organisations reported that attackers succeeded in encrypting data, with 44% paying the ransom to retrieve their data, a significant drop from 78% compared to the previous year.

However, despite paying the ransom, companies doubled their cost of recovery for the data held hostage by threat actors compared to organisations that did not pay the ransom and relied on backups.

Additionally, according to the Indian ransomware report released by India’s Computer Emergency Response Team (CERT-In),a 51% increase in ransomware incidentswas reported in H1 2022, with a majority of these attacks targeting data centres, IT, and TeS sectors in the country.

Threat actors tend to focus their attacks on organisations that hold valuable data. The more value the data has to the organisation and its stakeholders, the higher the chances that the ransom will be paid.

IT organisations and software vendors hold a lot of valuable data, including sensitive information like intellectual property.

If leaked by threat actors, it could lead to a drop in their value and replication of software, devaluing the company and threatening its revenue streams, making them a valuable target for cybercriminals. IT organisations providing cloud security and data solutions also hold large repositories of data for their clients. Successful attacks on them could potentially open the channel to target supply chains, adding pressure on companies to pay the ransom.

Data held by IT organisations could include personally identifiable data of clients’ users, intellectual property, access credentials, and even financial information. This data can be leveraged to launch further attacks. IT organisations are also among the first to adopt new technologies and encourage the use of open architecture, which may not have the highest levels of protection against cyberattacks, making them a target for cybercriminals.

Earlier this year, in November, a U.S.-based subsidiary of Infosys was reportedly targeted by a ransomware attack. At the time, Infosys McCamish Systems faced an incident involving a ransomware variant.

However, the company did not share details of the attack, stating that further information would be provided following a comprehensive investigation.

In March, Indian drug manufacturer Sun Pharma was hit by a cyberattack.

A ransomware group claimed responsibility for the attack, impacting the company’s revenue due to containment measures implemented to mitigate the damage.

In November 2022, a ransomware attack crippled the All India Institute of Medical Sciences (AIIMS) for days. Hackers reportedly demanded 200 crores in cryptocurrency from the hospital.

COMMents

SHARE

internet / cyber crime

BACK TO TOP

Terms & conditions | Institutional Subscriber

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Source : www.thehindu.com Date : 2023-12-28

UNJUST AND UNWISE: THE HINDU EDITORIAL ON COUNTER-INSURGENCY OPERATIONS IN J&K

Relevant for: Security Related Matters | Topic: Role of External State & Non-state actors in creating challenges to internal security incl. Terrorism & illegal Migration

December 28, 2023 12:30 am | Updated 12:30 am IST

In a conflict-prone border province such as Jammu and Kashmir (J&K), security forces have to tackle not only terrorism but also engage in counter-insurgency operations in a precise and just manner. The Pir Panjal Valley, comprising Poonch and Rajouri districts, has witnessed fierce encounters between security forces and militants in jungle terrain, leading to the death of 28 soldiers this year. The death of three civilians who were detained by the Army in the Poonch-Rajouri area following a deadly ambush on an Army convoy on December 21, and the fact that five other civilians were badly injured due to alleged torture by the security forces, is a severe indictment of the counter-insurgency tactics there. Such heinous actions by security forces targeting civilians in response to militant attacks are clearly problematic, on two counts. First, this increases the unpopularity of a regime that has not been democratically elected in the Union Territory where provincial elections have not been held for more than half a decade. This is a blow against counter-insurgency in an area that has been relatively more peaceful in comparison to the Kashmir Valley. In fact, the Pir Panjal region has been experiencing militancy in the last two years after relative calm for a decade and a half. Counter-insurgency operations of the kind that followed the ambush last week breed discontent among residents in a region which has not been supportive of militancy in the near past.

One of the aims of militants in the asymmetric warfare waged against Indian security forces is to provoke the forces into committing rights violations against civilians and to use grievances and indignation among them to increase their own support base. Such actions by security forces play into the hands of militants and their handlers across the border. Second, the legitimacy of force or violence and its use by the state depend on the justness of the actions. Indiscrimination in the use of violence targeting civilians without just cause only results in the questioning of that legitimacy in the eyes of the people. The J&K police have registered a murder case against unidentified persons following the deaths of the civilians and the Army has taken three senior officers off their posts while promising an inquiry. Both these agencies must now deliver justice quickly and in a firm manner. “Fake encounter” deaths and torture by security agencies in the Valley have resulted in spurts of increased militancy besides public outrage that developed into major law and order situations. The Bharatiya Janata Party-led Union government has tried to use a no-holds barred security-centric approach to tackle the problem of militancy and public anger in J&K. The repeated acts of rights violations and crimes in the name of counter-insurgency are clear evidence that this approach is not working.

COMMents

SHARE

Jammu and Kashmir / security measures / terrorism (crime) / human rights / police / Bharatiya Janata Party / government

BACK TO TOP

Terms & conditions | Institutional Subscriber

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END