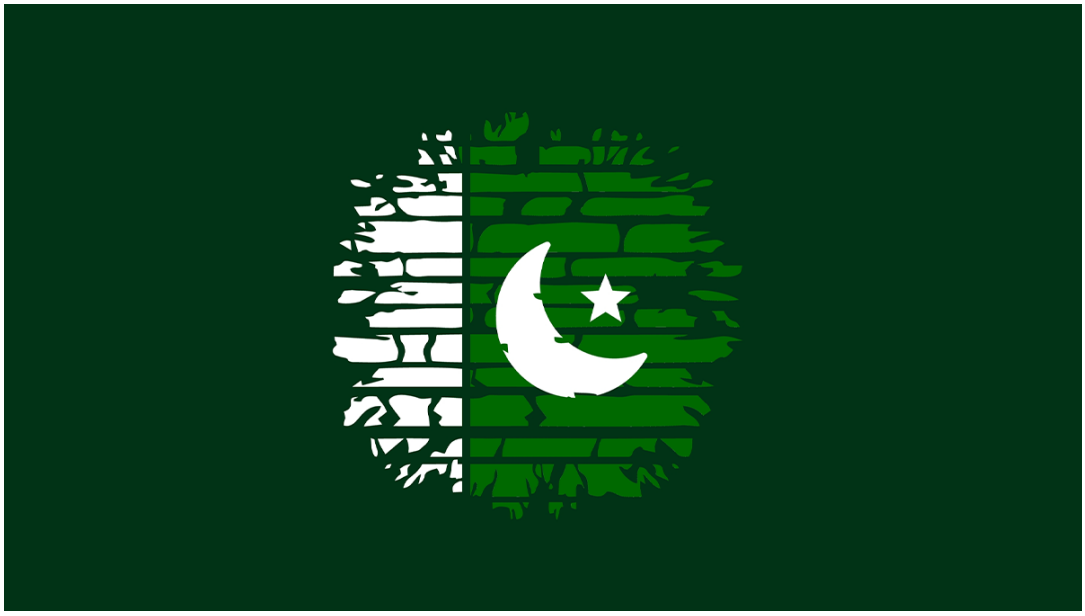
The Daily Swig
Cybersecurity news and views

Pakistan government approves new cybersecurity policy, cybercrime agency

Emma Woollacott 05 August 2021 at 10:33 UTC

Policy and Legislation | Cyber-attacks | Asia

New policy welcomed as much-needed improvement to 'poorly implemented' Prevention of Electronic Crime Act



The Pakistan Telecommunication Authority (PTA) has announced that a new cybersecurity policy and accompanying cybersecurity agency has been approved for the South Asian nation.

The new policy aims to support both public and private institutions, including national information systems and critical infrastructure, replacing a system whereby government institutions have separate security operations.

It comes at a delicate time for Pakistan, which recently accused India of using the Israeli spyware Pegasus to spy on Prime Minister Imran Khan – and designates cyber-attacks on any Pakistani institution as an attack on national sovereignty.

"The IT ministry and all relevant public and private institutions will be provided all possible assistance and support to ensure that their data, services, ICT products and systems are in line with the requirements of cybersecurity," said IT minister Syed Aminul Haq, as quoted in local press.

Shields up

Pakistan's new cybersecurity policy will include a new governance and institutional framework for a 'secure cyber ecosystem', along with computer emergency response teams (CERTs) and security operations centers (SOCs) at national, sector, and institutional levels.

And the policy calls for new information-sharing mechanisms, along with skills development and training programs and public awareness campaigns.

Read more of the latest cybersecurity news from Asia

"The cybersecurity policy announced by Pakistan is a welcome development," Javvad Malik, security awareness advocate at KnowBe4, tells *The Daily Swig*.

"Security awareness is essential. People need to be informed of the risks that come with interconnected systems, and what their role is in ensuring security. Once this groundwork is laid, then putting in place technologies and procedures to support these become easier and more effective."

Poor track record

Latest Posts

Orange Tsai documents exp against Microsoft Exchange
'Possibly the most severe vulnerab the history of Microsoft Exchange'

Attacking Let's Encrypt
Downgrade attack lowers the bar f printing fraudulent SSL certificates

'Shooting the messenger'
Dispute erupts between Chaos Co Club and Germany's CDU after da discovery

Pakistan has a poor record on cybersecurity, ranking 79th in the ITU's Global Cyber Security Index.

The country's current cyber law, the 'Prevention of Electronic Crime Act' (PECA), is poorly implemented, according to ethical hacker and security researcher Rafay Baloch.

"To quote a few examples, the federal government has yet to designate a digital forensics laboratory to provide expert opinion to the court independent of the investigative agency which is mandated by the section 40 of PECA," he tells *The Daily Swig*.

"Similarly, under section 49 of PECA, the federal government was required to designate national and sectoral CERTs for protecting against critical infrastructure."

ANALYSIS Iranian cyber-threat groups make up for lack of technical sophistication with social engineering trickery

Baloch says that the new policy should improve Pakistan's cybersecurity, in particular by harmonizing practices across different bodies.

"The major challenge pertaining to the policy is its implementation. A national cybersecurity policy is accompanied by a strategy document with an action plan to achieve the objectives laid out in the policy," he says.

"The strategy document would include prioritization of action items, timelines, roles and responsibilities of organizations responsible for implementing the objectives laid out in the policy."

He also calls for the government to develop an institutional framework consisting of dual civil-military agencies:

"That would be raised with the specific purpose of implementing the aforementioned policy objectives and maintaining national cyber defenses in government, commercial and military domains."

YOU MIGHT ALSO LIKE Research roadblock: Security pros weigh in on China's new vulnerability disclosure law

Policy and Legislation | Cyber-attacks | Asia | Pakistan | Hacking News | Government | Cybercrime | Cyber Warfare | Legal | Cloud Security | Network Security | Database Security | Email Security | Education

Emma Woollacott

@EmmaWoollacott

Related stories

Orange Tsai documents exploits against Microsoft Exchange

06 August 2021

Attacking Let's Encrypt

Downgrade attack lowers the bar for printing fraudulent SSL certificates

06 August 2021

'Shooting the messenger'

Dispute erupts between Chaos Computer Club and Germany's CDU after data leak discovery

06 August 2021

Enfilade

New tool flags ransomware and infections in MongoDB instances

06 August 2021