shaping tomorrow with you

FUJITSU

Cyber security: predictions for 2016

From mass breaches to targeted exploitation

2015 was the year of the breach. Cyberattacks exposed the systems of a huge number of large companies. So, what do you need to look out for in 2016? Armed with data, we expect cybercriminals to serve up highly targeted attacks.

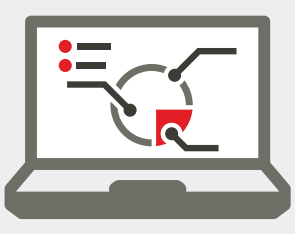
Read on to see our ten predictions for 2016. Are you prepared?

1

As the IoT grows, so will DDoS

Criminals will use connected, Internet of Things (IoT) devices to build botnets, creating a launchpad for damaging distributed denial of service (DDoS) attacks.

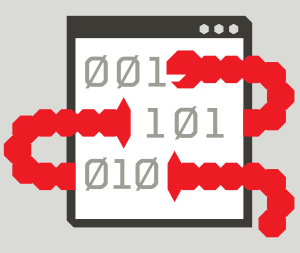
2



Data remains king

Attackers' hunger for data will grow. There are many ways they can exploit information – from extortion to identity theft. Companies with large amounts of personal data will be a target and will need to take action.

3



Web apps under attack

Hacking doesn't always require a lot of skill. Low level hackers will continue to use old faithful automated attacks such as SQL injection to target low hanging fruit. And this will increase in 2016.

4

Things are going to get personal

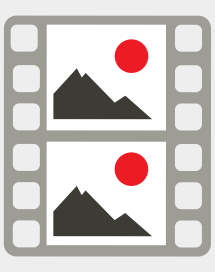
If cyber criminals get hold of sensitive images or personal data, they will hold individuals or companies to ransom. We expect this to happen more and more.

5

Biometrics on the rise

Passwords are easy to lose, hack or share. Companies will turn to biometric sensors to protect their data and their employees.

6



Flash in the spotlight

Hackers continue to use Adobe Flash as an attack vector to install malware. Businesses will start to decide if the media player is worth the risk in an enterprise environment.

7

The insider threat

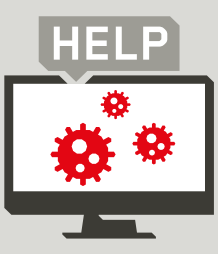
It might be malicious, it might be accidental, or it might be due to a tech savvy employee circumventing controls. But the risk of employees exposing data will grow.

8

Check the mail

Phishing is getting harder to spot. We think criminals will send post that appears to be from a real company. But it will direct the victim to a URL that contains malware. Look out for things like loan offers you didn't ask for.

9



Companies need expert help

Few companies will have the resources to keep on top of threats. To stay ahead, they will need to send their logs to specialist security providers.

10

https:// to become the norm

More websites will use the SSL/TLS protocol to serve web content more securely. But this will need to go hand in hand with interception technology to keep a check on inbound and outbound data or companies will have a huge blind spot.

Get the full picture

Our annual security report looks back at 2015. It then looks ahead to the threats we'll face in 2016.

Read the report >>

Think secure

We use Cyber Threat Intelligence to turn data into actionable intelligence – and make sure our clients have optimal protection. From our Security Operations Centres, we track the security of our clients' IT 24 hours a day. We're here to help today's businesses navigate the ever-changing landscape of cyber threats.

Visit our Secure Thinking website to learn more

shaping tomorrow with you

FUJITSU