Business Information

Technology insights for the data-driven enterprise

ALPHASPIRIT - FOTOLIA

MANAGE

1

IoT, edge computing spawn new security issues

As real-time big data increasingly hitches up to internet of things, edge computing power and fog nodes, a whole new layer of security threats emerges.

Scott Robinson, Lucina Health

Published: **09 Apr 2018**

In the beginning, the internet was created. It was thought to be good and evolved into internet of things that compute collected data out on the edge. Then, the edge begat fog computing, and the fog brought forth many new concerns about data security and privacy.

The breathe-in, breathe-out cycle of enterprise processing power -- that endless loop of centralize and decentralize that defined the past few decades -- has always heralded in new security paradigms. So as we watch IoT and edge computing morph into fog computing and as the enterprise necessarily becomes more dependent on mobile computing to get its daily chores done, we shouldn't be at all surprised to see yet another layer of security developing around us.

In simple terms, the more doors and windows that are placed in a building, the more breaking and entering avenues are created for thieves. Which begs the question: How are we securing all these doors and windows?

Sudden vulnerability as fog sets in

A brief Google search reveals that the biggest security threats to IoT, edge computing and fog computing come from distributed denial-of-service (DDoS) attacks -- the beating down of systems and applications by incessant IoT service calls. That's very predictable and was actually predicted with regularity by tech pundits over the past couple of years. According to Forrester Research, the biggest cybercriminal targets are government security and surveillance applications, retail inventory management apps and asset management in manufacturing.

Things will get worse before they get better: The sudden rise in such attacks obviously owes to their ease of deployment in a world quickly filling up with IoT devices. Juniper Research predicted that the number of connected IoT devices, sensors and actuators will hit more than 46 billion in three years.

But increased DDoS attacks are by no means the only increasing threat. Supervisory control and data acquisition (SCADA) systems are particularly vulnerable. They're increasingly essential to industrial infrastructure and key components in countless manufacturing systems -- and they must operate on IoT and edge computing protocols. They're difficult to update and often overlooked in IoT threat-scanning.

Similarly, newer cars and trucks are part of the fog computing ecosphere. They're simply great big

It would be difficult to overstate how pervasive and permanent these new concerns will become. We're in a brave new world now. As IoT continues to grow in the coming years, the integration of all things that compute is destined to become an embedded reality of enterprise business strategy and resource management.

So, what can be done?

Trustworthy IoT, edge computing trinkets

Another prediction that's coming true is that OEMs will scramble to address the security concerns surrounding their offerings. For example, the Trusted Platform Module (TPM) -- a secure microcontroller with added cryptographic functionality -- is being deployed at the hardware level. Cryptographic keys are embedded in the chips of IoT devices to facilitate authentication. IoT devices therefore can be secured by avoiding the mistake of sharing the keys on a bus and keeping encryption and decryption within TPM.

Another proactive step is ensuring encryption in IoT local communication. IoT devices are endpoints that integrate with their parent systems via edge gateways. Even though we may not think of them in that way, it's important to treat those endpoints as foreign. All IoT and edge computing gateways need to be independently secured -- most commonly by X.509 certificates.

Raise your own chickens

Jack LaLanne, the original fitness guru, once insisted that he would never consume a food whose origin was unknown -- and that extended to eating his homegrown chickens. Edge and fog computing poses a metaphorically similar challenge: When a company parses out computer power beyond its own borders, it's often handing off to resources that aren't homegrown and are therefore not necessarily secure or trustworthy.

The true suck-it-up factor is the need for continuous updates of all the parts and pieces on a level never done before.

The main player in this hand-off is commonly called a *fog node*, a kind of mini cloud of processing resource beyond the enterprise boundary. Offloading to fog nodes makes the integration of inbound IoT and edge computing data far more efficient and stretches global search -- a mixed blessing because it creates more vulnerabilities. That in turn creates a new requirement -- *verifiable computing* -- to ensure that the processing conducted in potentially untrusted servers or devices attains the confidence level it should.

A number of verifiable computing strategies are emerging as this new paradigm takes hold. One is the implementation of a verification protocol that maintains client privacy of data input and output involving fog servers and devices. Another strategy is client verification of fog node processing via a public evaluation key, which generates a proof of correctness on the front end of the client-server exchange.

As for global search, sensitive data from end users must be encrypted before outsourcing to a fog node, which can create difficulties. If the data needs to be searched via keyword, a searchable encryption scheme must be implemented. It's a nuisance, but it's the world we live in. Facing this challenge will trigger new evaluations of what data should and shouldn't reside in fog nodes.

Continuous lifecycle management

The true suck-it-up factor is the need for continuous updates of all the parts and pieces on a level never done before.

Upgrades and patches -- long the bane of enterprise IT -- are now more essential than ever. The firmware of these devices out on the edge represents a care-and-feeding requirement that's more mission-critical than the upgrading and patching of the laptops, desktops and servers back at headquarters. We've gotten very good at keeping things tidy in-house; we must, whether we like it or not, be even tidier out in the world.

Scott Robinson asks:

What security actions are you taking to protect your data edge?

Join the Discussion

Article 6 of 6

Next Steps

AI for IT connects operations to Oracle ERP

Dig Deeper on Data quality management software

A glossary of the IoT terminology you must know

By: Kristen Gloss

fog computing (fog networking, fogging)

By: Margaret Rouse

Fog nodes simplify edge vs. cloud computing choice

By: Scott Robinson

Get to know edge storage and the technology around it

By: Stacey Peterson

Join the conversation

1 comment

Share your comment

Send me notifications when other members comment.

Create Username and Add My Comment

Oldest ▼

[-] **ITKE**

- 9 Apr 2018 1:17 PM

What security actions are you taking to protect your data at the edge?

Reply

Get More Business Information

Access to all of our back issues

2018

E-Zine | Dec 2018

E-Zine | Oct 2018

E-Zine | Aug 2018

E-Zine | Jun 2018

View All

SearchBusinessAnalytics

Big data streaming platforms empower real-time analytics

Data streaming processes are becoming more popular across businesses and industries. Read on to see how streaming platform ...

Coronavirus quickly expands role of analytics in enterprises

While NLP and embedded BI were expected to be key analytics trends, the effect of the pandemic on enterprises' takeup of ...