ISSA
Information Systems Security Association
Greater Kansas City Chapter

Volume 63, Issue 2 The Newsletter of the Greater Kansas City ISSA Chapter February 2019

The President's Corner

Inside This Issue

Hope you all enjoyed the January presentation. I thought the hack demo was very insightful on how easy it is for a bad actor to get into your phone. This month i am looking forward to "Patch Smarter not Harder" topic by Kenna Security.

Do you know you can access upcoming ISSA international Web presentations via https://www.issa.org/page/WebConferences

If you have topic you like to see, please let us know and we will try to get the presenter. If you would like to serve ISSA KC as a board member or committee member, please reach out to me at president@kc.issa.org.

Sincerely,
Naeem Babri
President, ISSA-Greater Kansas City Chapter

Upcoming Events

Chapter Meeting

February 28, 2019
Topic: *Patch Smarter, Not Harder*

Chapter Meeting

March 28th, 2019
VMware

Connect With Us
kc.issa.org

Twitter
KansasCityISSA

Facebook @kcissa

LinkedIn

The Information Systems Security Association (ISSA) is an international organization providing educational forums, publications and peer interaction opportunities that enhance the knowledge, skills and professionalism. The primary goal of ISSA is to promote management practices that will ensure availability, integrity and confidentiality of organizational resources.

Chapter News

ISSA Journal : Feb 2019

Feature articles include:

- California Dreaming - The Fight with the Federal Government over Technology
- Bridging the Cyber Gap: Spotting Hidden Security Talent in Your Organization
- SIEM Implementation for School Districts Utilizing FOSS
- Automation of Business-Aware Incident Management

Members: please click on the following Journal issue links for access: Computer: Bluetoad - PDF; Mobile: ePub - Mob

Not a member? Read this month's feature article - The Future of IT Risk Management Will Be Quantified - at no charge or Join Now and gain full access to the *ISSA Journal*.

Webinars & Conferences

RSAConference | Where the world talks security

Infinite cybersecurity impact.

You've heard about it. Probably read about it. And now's your chance to live it.

RSA Conference **2019** is the place to be for the latest in cybersecurity data, innovation and thought leadership. From **March 4 – 8,** San Francisco will come alive with cybersecurity's brightest minds as they gather together to discuss the industry's newest developments. And predict what's to come in the year ahead. From keynotes presented by your favorite experts to endless sessions covering everything under the cybersecurity sun, there's truly no better place to refresh your insights and connect with peers from around the globe. Register, https://www.rsaconference.com/events/us19/register

---

KANSAS CITY BSIDES

BSides KC 2019 on Friday and Saturday, April 26-27, 2019

Plexpod Westport: 300 E 39th St, Kansas City, MO 64111

https://www.bsideskc.org/

THE WIT NETWORK

International Women's Day March 8th, 2019

A global day celebrating the social, economic, cultural and political achievements of women. The day also marks a call to action for accelerating gender parity.

https://thewitnetwork.com/international-womens-day-conference-2019/

Save the date! May 8, 2019

7th Annual SecureWorld Kansas City, Cybersecurity Conference, Overland Park Convention Center

Information and ISSA Discount link: **ISSA KC**

Conference Agenda

Upcoming Chapter Event

Feb 28, 2019 the ISSA KC Chapter Meeting

Topic/ Presentation Overview:
Patch Smarter, Not Harder. In this talk, we will discuss why most organizations are wasting time and resources by patching the wrong systems on their networks and how taking a data-drive approach based off threat intel helps you decide what needs to be prioritized.

Speaker Bio:
Jerry Gamblin is the principal security engineer for Kenna Security. He is an industry recognized visionary with high-caliber talent in directing all aspects of highly technical security initiatives and transformative projects. He is an internationally known speaker, writer, security researcher, and blogger.

Location:
Brio on the Plaza
502 Nichols Rd, Kansas City, MO 64112

Agenda:
11:30AM -12:00PM - Registration and Check In
12:00 PM -1:00 PM - Lunch
1:00 PM - 3:00 PM - Speaker's Presentation

KENNA Security

Price:
$25 members| $30 guests

CPE's: 1 Credits *Please note actual CPE hours granted are dependent upon duration of speaker's presentation and may differ from advertised number of CPE hours.

We look forward to seeing you at the event. If you have any questions about the event or how to register, please email our RSVP email, or contact the venue for directions.

Register

Next Month
March 28, 2019 the ISSA KC Chapter Meeting

Topic: Coming Soon!

Location: Hereford House
5001 Town Center Drive
Leawood, KS 66211

Agenda:
11:30AM -12:00PM - Registration and Check In
12:00 PM -1:00 PM - Lunch
1:00 PM - 3:00 PM - Speaker's Presentation

vmware

Price:
$25 members| $30 guests

CPE's: 1 Credits *Please note actual CPE hours granted are dependent upon duration of speaker's presentation and may differ from advertised number of CPE hours.

Membership

We like to welcome new member Paul Kuhl! If you have any questions about membership please contact Wai Cheng.

I like to share a Password check up article, Google's Password Checkup Chrome browser Extension
https://www.blog.google/technology/safety-security/google-password-checkup-cross-account-protection/

Best Regards,
Director of Membership
Wei Cheng

Security & Privacy: Articles and News

Feature Articles

Wicked (dark web) wish list

By -Bradley Barth

The dark web can be a fairly lawless place, but even the most hidden corners of the darknet are not immune to the laws of supply and demand.

Malware programs, cybercriminal services and stolen data can skyrocket in popularity on the underground market just as quickly as they can fall out of favor – same as any product sold in the legitimate economy.

A couple of black market cyber trends truly took off in 2018 with experts predicting a few new ones will spring up in 2019.

Malicious software and services

It happens all the time: A pioneering hacker or sophisticated threat group becomes the first to introduce a new malware or exploit – and suddenly a whole clowder of copycats emerge. As demand for these malicious tools grow on the darknet, developers and buyers begin to offer the same functionality – sometimes in the form of malware, other times as malware-as-a-service.

*** Continued

Batten down the DNS hatches as attackers strike Feds

By - -Michael Cooney @ Network World

If enterprise IT folks haven't taken a look at their DNS ecosystem recently now may be a good time.

This week the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) told all federal agencies to bolt down their Domain Name System in the face of a series of global hacking campaigns.

DNS, routinely known as the Internet's phonebook, is part of the global internet infrastructure that translates between familiar names and the numbers computers need to access a website or send an email.

CISA said in its Emergency Directive that it is tracking a series of incidents targeting Domain Name System (DNS) infrastructure. CISA wrote that it "is aware of multiple executive branch agency domains that were impacted by the tampering campaign and has notified the agencies that maintain them."

CISA says that attackers have managed to intercept and redirect web and mail traffic and could target other networked services. The agency said the attacks start with compromising user credentials of an account that can make changes to DNS records.

*** Continued

Mentor Program: ISSA Greater Kansas City

The program is designed to formalize relationships between senior professional individuals in the chapter (Mentors) and the various levels of security professionals seeking entry or moving through the different phases of this profession (Mentees). There are many different types of mentoring partnerships; peer to peer, adult to adolescent, apprentice to master, cross generational, and mentoring within a company or a few. It depends on what type of mentoring relationship you're seeking.

Mentor/Mentee application: Mentor Application :: Mentee Application

Feature Articles - continued

Continued News from Article Page

OWASP's top 10 IoT vulnerabilities -

-By Fredric Paul, Network World

Everyone knows security is a big issue for the Internet of Things, but what specifically should we be most afraid of? OWASP identifies the top 10 vulnerabilities.

To that end, on Christmas Day, OWASP released its top 10 IoT vulnerabilities for 2018, complete with an infographic (see below). Let's take a look at the list, with some commentary:

1. Weak, guessable, or hardcoded passwords

"Use of easily brute-forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems."

Frankly, this issue is so obvious that I can hardly believe it's still something we have to think about. I don't care how cheap or innocuous an IoT device or application may be, there's never an excuse for this kind of laziness.
[Prepare to become a Certified Information Security Systems Professional with this comprehensive online course from PluralSight. Now offering a 10-day free trial!]

2. Insecure network services

"Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control."

This makes sense, but it's a bit more of a gray area, as it's not always clear whether those network services are "unneeded or insecure."

3. Insecure ecosystem interfaces

“Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.”

Again, it’s not always obvious whether the interfaces are actually allowing compromise, but authentication, encryption, and filtering are always good ideas.

4. Lack of secure update mechanisms

“Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.”

This is an ongoing issue for IoT applications, as many vendors and enterprises don’t bother to think through the future of their devices and implementations. In addition, it’s not always a technology issue. In some cases, the physical location of IoT devices makes updating—and repair/replacement—a significant challenge.
[Read also: What happens when an IoT implementation goes bad?]

5. Use of insecure or outdated components

“Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.”

Come on, folks, there’s no excuse for this kind of problem. Stop being cheap and do things right.

6. Insufficient privacy protection

“User’s personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission."

Obviously, personal information needs to be dealt with appropriately. But the key here is “permission.” Almost nothing you do with someone’s personal info is OK unless you have their permission.
[Read also: People are really worried about IoT data privacy and security—and they should be]

7. Insecure data transfer and storage

“Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.”

While many IoT vendors pay attention to secure storage, making sure data remains secure during transfer is too often ignored.

8. Lack of device management

“Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.”

IoT devices may be small, inexpensive, and deployed in large numbers, but that doesn’t mean you don’t have to manage them. In fact, it makes managing them more important than ever. Even if that’s not always easy, cheap, or convenient.

9. Insecure default settings

“Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.”

Sheesh. Another problem that shouldn’t be happening in 2019. Everyone knows this is an issue, and they know how to avoid it. So, let’s just make it happen… every time.

10. Lack of physical hardening

“Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.”

The IoT is made up of “things.” This shouldn’t be a surprise; it’s right there in the name. It’s important to remember the physical nature of the IoT and take steps to secure the actual devices involved.

*** Continued

Sponsors

Board of Directors

President
Naeem Babri

Secretary of Board
Rochelle Boyd

Treasurer
Gary Kretzer

Director of Membership
Wai Cheng

Director of Education
Nicole Windholz

Director of Programs
Chris Mcleod

Webmaster
Thomas Badgett

CISSP Study Group
Mark Waugh

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood
Michelle Moloney

Our Sponsors

viawest

CARBON BLACK

CYBERARK

Integrity

proofpoint.

CRITICALSTART

okta

Zerto
IT RESILIENCE

SECURONIX

FORCEPOINT
POWERED BY Raytheon

McAfee