Patti Perspective

July 2011 - Vol. IV, Issue 2

Quick Links

Patti Engineering's website

Patti Engineering's Blog

President, Sam Hoff's Blog

V.P. of Engineering, Dave Foster's Blog

Like us on Facebook

View our profile on LinkedIn

View our videos on YouTube

Follow us on twitter

Greetings!

As the month of July comes to a close and the heat wave that has lingered over most of our country has moved on, we are bringing you a hot topic this month. This is a must read and it is certainly not the kind of hot topic that you will ever want to have to address in your business. This sort of hot topic could shut down your business with chilling effects on your bottom line. The hot topic is the ***Stuxnet Virus.***

This is a virus currently circulating that activates an unusual kind of malicious software attacking floor level control systems, which some analysts describe as 'corporate espionage'. I have to hand it to our Vice President of Engineering, Dave Foster, he has done a great job writing this article to make it clear, to even the layman, exactly why and how this virus can cripple a plant floor.

Patti Engineering's team of engineers have the training and expertise to address the dangers imposed by the Stuxnet and other viruses, we offer security audits to insure our clients are protected. If you would like to learn more after reading the article, please reply to this email or call our office at 1-800-852-0994 (US Only) or (248) 364-3200.

On a much lighter note, after you take in the interesting article written by Dave Foster, please see our employee highlight section where you will learn about our talented Senior Engineer, Steve Palmgren, who made the big move from Michigan to Texas to lead the engineering team in our growing Texas office.

Best regards,

Georgia H. Whalen
Director of Marketing
Patti Engineering
Phone: 978.697.2664
email: gwhalen@pattieng.com

Industrial IT Security can no Longer Rely on Just Fortress Building

*This article was written by Patti Engineering Vice President, Dave Foster.*You can e-mail Dave with questions or comments at: DFoster@PattiEng.com.

The Stuxnet Virus has opened our eyes. As more and more IT based devices have made their way into industrial settings, the protection of these devices from those wanting to do harm has not kept up the pace. In the front office environment, many layers of protection technologies have evolved, but in the industrial environment we have hung on to just one tool. Build a BIG wall; a fortress.

History has many lessons on this. China built a long one that spanned almost the width of their nation. The Europeans made an art form out of building tall encompassing ones (the Royal Family's Windsor castle in England is a great example of this). But these alone proved to not be enough to thwart every intruder. They had to start getting creative. They added arrow slit openings in the wall

to deter low level attacks, and watchtowers to see the siege arriving. They added ditches or moats at the base of the walls to keep enemies from climbing or digging under them. They discovered defense in depth. Break through one defensive strategy and the next one is there to greet you (rather impolitely, of course).

The Stuxnet virus was created for a singular purpose. It attacked the Siemens S7 PLC and their WinCC SCADA software. But all the mechanisms it used to get there make EVERY industrial system from EVERY industrial manufacturer vulnerable. It easily found ways around the existing "great wall" of IT security systems by hitching a ride on USB memory sticks. It exploited common vulnerabilities in the Windows environment, and was smart enough to remove itself after only 3 replications - to avoid detection. It learned things as it went, as well. Each iteration was remembering how its previous iterations got there, learning your whole network along the way. It was very patient as it cruised along until it ultimately made it to the programmed target. It would not take much effort to change that target to any number of other industrial devices. And while the USB stick was a convenient choice for transport, people have even found ways to embed this virus into a PDF file. Wireless connectivity is also a serious concern for intrusion. The wall is almost useless by itself when the intruder gets walked through the door.

The argument used to be made that there was an "air gap" between the industrial devices and the obviously vulnerable front office devices that were all connected to the rest of the world. But that is mostly gone in today's world of interconnectivity and open platforms. Industrial devices protected solely by strict IT policy or singular firewall equipment that says "nothing gets past my wall" have proven to be vulnerable. While good IT policy is essential, the policies that govern PCs sitting on an accountant's desk do not work on Automation Control Systems. It takes a collaborative effort between IT and operations to develop an effective policy for defending your floor level control systems.

There is a growing contingent of hackers out there that see opportunity and potential "pay days" by taking out the competition, or want to make a statement against corporations. Do you think that you will never be a target of these hackers? Up to 80% of the Stuxnet virus infections were collateral damage, not even the intended target. Now is the time to take a look your "defense in depth" strategy for IT security in your industrial environment, before it is too late. Give us a call!

Phone: 1-800-852-0994 (US Only)
(248) 364-3200

csia control system integrators association CERTIFIED

Solution Partner
Automation
SIEMENS

Patti Personnel - Steve Palmgren

Patti Engineering's business is growing at a fast pace in Texas. Steve Palmgren's outstanding engineering talent and leadership skills have been instrumental in driving our growth in the Texas market.

Steve Palmgren holds the position of Branch Manager/Senior Electrical Controls Engineer and currently manages our Austin, Texas office. Palmgren has been with Patti Engineering since 2001 and has 14 years of experience in control systems integration. His responsibilities include: hardware and software design, control engineering and project management.

Palmgren has been the lead engineer on several of Patti Engineering's most significant projects with our most visible clients. In addition to completing numerous training courses, he earned his bachelor degree in electrical engineering with a minor in computer engineering from Kettering University in Flint, Michigan.

Steve and his wife Lindsay have one daughter, Reese. The Palmgren family enjoys spending time outdoors enjoying many of Austin's live music venues, parks, and pools. You will commonly find Steve tinkering or fixing something in his garage in his free time. Steve is also an avid College Football fan.

The Palmgren Family

On a fun note, we thought it would be interesting ask Steve to summarize how he, Lindsay and Reese have adjusted to their big move south to the Lone Star State. Steve provided us with interesting insights:

We are still adjusting to the hot Texas climate after both growing up in Michigan. However, we are starting to feel more at home in Austin after 1.5 years. We really enjoyed this past winter and not having to shovel snow and scrape ice. The one day it snowed about 1 inch of snow, we didn't mind at all. It was so worth it to get out (our car is a 4x4, not that we needed it for 1 inch of snow) and see almost nobody on the roads and most major businesses closed. We saw many people that forgot to turn off their sprinkler systems and had a yard full of ice. We also decided to head to Ikea later that day to do some shopping to find that Ikea was "Closed due to inclement weather". We looked around. It was 45 degrees F, sunny, and no snow or ice to be found. It had all melted by noon. Nevertheless, Reese was disappointed she couldn't have meatballs for dinner.

We have been corrected on several Midwestern phrases and pronunciations... Y'all instead of you guys. Pecan (pah'con) instead of pecan (pee'con). Cement (SEE'ment) instead of cement (Sa'ment). And especially many of the local Austin names. Most recently I was working in Calgary for a client from Austin. My client's customer, asked me at some point if I was from their Calgary office. I responded "No, I'm from Austin, like the other guys. Why do you ask?" They responded "We'll you don't sound like you are from Texas..." I laughed and explained that I grew up in Michigan and have lots of family in Canada.

Overall, we are enjoying Austin and everything is has to offer. Everyone is so friendly and easy going. The only bad thing we can say about Austin is all of our family and many of our good friends are back in Michigan. We do try to get back to Michigan to visit when we can and we have also been lucky to have had family and friends come to visit us as well.