CyberPro

Volume 7, Edition 9
May 1, 2014

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Mark Zalubas, Vice President of Solutions Engineering, Merlin International

NSCI recently had the opportunity to interview Mark Zalubas, Vice President of Solutions Engineering for Merlin International in Vienna, VA, where he is responsible for architecting and developing next-generation IT solutions for federal agency clients. With a career spanning over 20 years, Mark has served in a wide range of engineering and marketing positions with a variety of government-focused and commercial companies, including: General Electric Aerospace/Lockheed Martin, Oracle, Enterworks, Convergys, Avise Solutions, and Cybertap. Mark's areas of expertise include cyber security, software systems engineering and architecture, database development, human factors engineering, SOA and middleware, and contact center/customer experience optimization. His experience, in all facets of a product offering, ensures quality solutions and enhanced value are delivered to every customer. Mark holds a Bachelor of Science in Aerospace Engineering from the University of Maryland and a Master of Science in Systems Engineering from Virginia Tech.

NSCI: Can you first tell us a little bit about Merlin International and its niche in the cyber market?

Zalubas: Merlin is a provider of comprehensive infrastructure, performance optimization, enterprise applications, and cybersecurity solutions to the Federal government. Our use of the word *comprehensive* means that we address any and all relevant factors to include products, both software and hardware; labor, both development and O&M; staging, financing, and retirement of the old system. Merlin has always had a number of security products in our portfolio, but our cybersecurity focus really took off when our largest customer, the Department of Veterans Affairs, undertook a major security initiative to secure and monitor its infrastructure. Merlin, being a veteran-owned company, takes great pride in being able to make a difference at VA for our nation's veterans and we jumped into the cybersecurity products market with both feet. Our products have always led to development and deployment engagements and from there we acquired a reputation in the cyber space, which took us into HHS's CSIRC (Computer Security Incident Response Center) in a security operations role. Our strength lies in crafting and delivering creative cyber solutions that optimally address all factors.

NSCI: When it comes to cybersecurity, how do you see the balance between people, processes, and technology?

Zalubas: I see these as ingredients that we use to craft our solutions, but I do think this age-old list is somewhat limiting. One item that I think is missing is data or intellectual property. It is the life-blood that runs through all elements of any solution. This IP can be the processes themselves, the rules being executed on an IPS (Intrusion Protection System) or SIEM (Security Information Event Manager), the conditional formatting that colors an incident red vs. yellow and increases our responsiveness and on and on. Solutions tend to be full of IP and it is what tailors a solution uniquely to one customer over another and also what differentiates a good solution from a bad one. I want the broadest set of ingredients when crafting a solution, so I don't limit myself by what ingredients that I can and cannot use. As long as I am hitting the customer's objectives across all important factors then the solution is correctly aligned.

NSCI: What are a few of the key cyber-related technology challenges you see in the future?

Zalubas: In the short term I see the industry and its vendors maturing rapidly, which means that anything you build today will be out-of-date more quickly than you'd like and you'll feel like you are constantly rebuilding. It is just a function of where we are in the maturation of the cyber vertical. To me, this feels akin to when the web exploded and new technologies (like application servers) and standards (like HTML and XML and Java) were evolving as quickly as they could, but they were always behind what was needed at the time. Now we have more stable technologies for the web that enable us to do what we need and over time, we will see this in the cyber vertical too.
In the longer term I see a massive increase in the amount of data that will be gathered, monitored, and processed. As we close the main door, the hackers will attempt to come in one of the windows. We'll cut off every avenue we can think of and eventually they'll find a way to come in the smallest unprotected pore of a system. This will result in ever-more data being generated and analyzed to ensure security. We will need the tools to be able to handle this exponential increase in data as we continue to look at each level more granularly than in the past. We will need to be able to process and understand this data, and since it is all new territory there won't be any guides to help.

NSCI: The healthcare industry and financial industry seem to be competing for the most data breaches. What key technologies do you think would help these industries the most?

Zalubas: They both have something valuable to protect so it makes perfect sense that they would be hit more often than other verticals. Without knowing their specific needs, I would offer that segmenting all IT assets (data included) into categories that require more or less security, permits additional protection to be applied to the most critical items instead of attempting to protect everything equally. You want an armored car to pick up your money from the restaurant, but it is OK for a linens service to pick up the tablecloths with just an ordinary truck. Assigning criticality is key to making this happen online like it does in the physical world.

NSCI: There's a lot of talk about improving software development processes to ensure security is built in up front. How do you balance this with time and funding constraints, and sometimes lengthy government processes (e.g. requirements, acquisition, fielding)?

Zalubas: Security really is just another requirement type so it has to be built in from the start, but not everything has to be done within the application. Many cyber products, such as identity managers, firewalls, and XML gateways, perform functions that in years past had to be built into every application again and again. Now, we have achieved truly distributed architectures and most applications are really 'virtual systems' composed of collections of existing services, COTS, and custom-built objects and services. Instead of being built in to applications, security needs to be incorporated into the virtual system design using what we hope will be available mature security elements and not have to be built each time. These identity management, authentication, and authorization technologies have been around for a long time and tend to be some of the more mature cyber technologies on the market today. The newer cyber technologies tend to address monitoring ever more granular network and platform items and assessing behavioral changes in users that might signal something. Another element helping this is the death of large-scale waterfall developments in lieu of smaller agile methodology efforts. With so many applications already written for most common tasks and COTS products addressing almost anything you can think of it is less and less frequent that the government is contracting for long-term, thousand page requirements style systems. More often the procurement involves iterating existing code every 3-4 weeks in support of changing mission requirements. This change in development philosophy has mostly eliminated the lengthy government processes you referred to.

NSCI: There's been a lot in the press on the inadequacy of cloud security. What are your thoughts?

Zalubas: Clouds are relatively new. We want to trust them but there isn't much of a track record yet. There have been some significant cyber break-ins at some institutions that you would think would spend anything to ensure that they didn't happen but it did. I think everyone is taking a wait and see attitude. They don't want to be the news story. This is where the segmentation of data into criticality makes a lot of sense. Why go to the cloud with your most critical data first? If it is all mixed together then you have no choice since going to the cloud means going with your most sensitive data. Why not try it with data that is the least sensitive. Then if it gets hacked you haven't actually compromised anything. If the linens truck gets robbed you don't really care, but you would if the armored car got robbed. The FEDRAMP program is helpful since it gives everyone a yardstick to measure themselves against and gives the government confidence that everything we know to do has been done, even if it leads to a compromise. FEDRAMP means that you aren't out there alone defending your assessment of how good the cloud security really was. You have some standards folks on your side. We'll all be there eventually.

NSCI: Let's talk about the insider threat. What are some practical steps organizations should take to prevent and/or limit the damage?

Zalubas: I'm going to go back to something I said a number of times above. Segment the criticality of your data and spend more time watching and protecting the more critical information. Also, take the time to understand what roles in your organization need access to what data, and then be able to monitor or trigger events when access outside the desired user group is happening. I do see this as being a huge growth area for cyber solutions since insiders have much more ready access to everything and, at least currently, are less suspected than outsiders. I have noted recently some interesting cyber technologies that can encrypt your documents and require a key that is retrieved upon opening the document. If the document is stolen and the thief attempts to open the document it will call home for the decryption key and won't be issued it because of the location the request is coming from. This can be another ingredient is securing more critical data.

NSCI: We see an increase in people mentioning the "Internet of Things". How is this going to differ from the Internet we have today? What challenges should organizations and/or individuals be preparing for?

Zalubas: The Internet of Things will have so many more devices, thus adding to the big data collection, monitoring, and analysis challenge I referred to earlier. Like with anything, there will be both well and less well built products. Those built less well will be more likely to contain spaces in which malware can hide and operate from. Monitoring all of these spaces will require many unique connectors and tools to ensure security across the board. Hopefully standards will be set and adhered to so that the Internet of Things doesn't become the Internet of Problems, but rather the Internet of Good Things.

NSCI: Is there anything else you'd like to add?

Zalubas: I think I'm good. Thanks for the opportunity and thoughtful questions.

NSCI: Thank you very much for taking the time to visit with us.