Brent Huston is the CEO and Security Evangelist at MicroSolved. Brent is an accomplished computer and information security speaker and has published numerous white papers on security-related topics.

Unlike what I'd call a "regular CEO" you enjoy quite a bit of technical tinkering and dwell into security research. What drives you?

I was a technician to start with. I have always been a technical security guy and spent my early years at MicroSolved doing hands on penetration testing, exploit development and security research. I guess you could say I grew into being the CEO after we hired a person to be the CEO and he left the company 28 days later. It was a necessity that someone do it, so I took it on. That led me to a focus on growing my marketing and leadership skills as well as my technical skills.

My wife would say it made me a "more rounded person", but the truth is, I enjoyed learning the business skills as much as reading packet dumps. I really like helping management and board folks understand the real world threats in their own language and I am very happy that that has proven to be a talent of mine.

How does the technical aspect fit into your responsibilities as the CEO?

These days I split my time between marketing, leadership and technical research, primarily focused on our HoneyPoint line of products for security visibility. The good news is that those technical threat vector insights has helped us grow MicroSolved, since we bring some unique knowledge and capabilities to our clients that stem from our in depth exposures to bleeding edge attack techniques.

How would you assess the current state of Internet security threats?

I think the state of the OS and networks, in general is much improved. Some of the very basics we talked about for years (firewalls, patching, etc.) are starting to become mainstream and common practice. I think security at the application layer and designing for failure are currently the biggest challenges. I think our industry has a lot of bad habits.

We rely on user awareness to solve problems that awareness won't solve, like malware. We also tend to engineer IT environments and applications as if best practices were in place, when in reality, they rarely are. We need to embrace the idea that designing for failure is much more real world than designing by best practice. We know, from experience, that failure happens - thus we have to design our systems, networks and applications to minimize the damages that failure can cause. Again, malware as an example, if we know that some user will click on the dancing gnome and get a nasty infection, then we have to design user IT environments and server/data connectivity in such a way that we maintain confidentiality, integrity and availability even when some machines in the user base are compromised. Ideally, we would continue to strive for prevention, but increase our capabilities in detection by moving away from heuristics and identifying abnormal behaviors and then create automated responsive processes that allowed components in the IT environment to defend themselves while humans enable greater controls and take deeper protective actions. Until we can embrace this type of security at the system, network and application level, attackers will continue to have the upper hand.

We rely on user awareness to solve problems that awareness won't solve, like malware.

What type of developments do you see ahead?

What keeps me up at night is embedded devices and their applications. We have just seen malware that turns small modems and routers into bots, but what happens when the blender, coffee maker, refrigerator and your house are all "smart" components? We have already seen small scale infections of automobile computers and cell phones, so what kinds of embedded targets are we creating every day? From the "smart energy grid" to our dependence on our cell phones and from embedded network devices to "smart appliances", we are going to see a world where all things are connected and all things are a target. Malware at the embedded level may well be the scourge of information security when the young professionals we are mentoring today reach the season of their careers. Such attacks and infection capabilities could make bots seem "nostalgic" like some of us look upon defacements of days gone by today.

Of course, that said, there is good news here, too. The future is not all about fear. We are getting better at designing for security. We will likely create much more secure applications and computing platforms in the future. Even while attackers continue to evolve their craft, so too do the developers, programmers and engineers. There will be new bugs, for sure, but there will also be innovations in protective technologies that help reduce our overall exposures to these technical risks.

What do you see as the areas of true innovation when it comes to computer security?

I really hope that people move away from signature-based technologies. Today, when I do forward looking talks, it is usually around the two core ideas of finding new ways to design/engineer for failure tolerance and the idea that behavioral detective tools are much smarter. We know what attackers do and we know how they behave. There are really very few "game changing" attack techniques. This was the reason I built HoneyPoint in the first place. We have created a toolset around the ideas of capturing and detecting behaviors that normal users don't or shouldn't do, but that we know fit common behaviors of malware or human attackers.

I am a strong believer in the idea that we have to turn the tables on attackers and take away their ability to act with confidence. If they can't scan the network for targets, that reduces their target set. If they can't access data on the servers and workstations because they don't know which ones are real and which ones are HoneyPoint Trojans, then their capabilities are reduced again. If they are sniffing the network and our HoneyBees are putting fake credentials on the wire, then they

don't know what accounts are real and what ones will trigger alerts. Basically, we keep chipping away at their capability to know what is real and what is a trap until they become significantly less of a risk because we have reduced their options drastically.

You are very active both on Twitter and on your blog. How have these means of communication shaped the way MicroSolved does business?

Twitter and other social networks have been great for us. We are big fans of Seth Godin and the idea of building a tribe. We have been able to grow the business even in down economies because we have focused on the idea that every single thing we do needs to bring value to customers and the tribe in general.

Our partners often say that we are too focused on the clients and that we give away too much software, knowledge and tools for free. We feel just the opposite, that the customer has to be the focus and that value is real way that we earn their trust. Twitter and other social networks, the stateofsecurity.com blog and all of the public education, pro-bono work and stuff we do are the keys that unlock the true value of our relationship with our clients and the tribe at large.

I think every CEO should talk to customers as much as possible. I think too many CEOs are locked away from the public and their client base.

Should more CEOs take a moment to talk to their peers and customers this way?

I think every CEO should talk to customers as much as possible. I think too many CEOs are locked away from the public and their client base.

You have to be engaged with them, you have to work in the trenches with your tribe and at the same time have enough vision to make strategic decisions. I don't think enough companies operate this way. I treasure hearing from clients and having them pull me aside for conversations. I love hearing from them on twitter or through the blog. Heck, unlike some other CEOs, you can even call me on the phone. Clients are the center of MicroSolved and I wouldn't have it any other way!

You recently released HoneyPoint Personal Edition v2. How long did the development process take?

Going from 1.0 to 2.0 took about 30 days of development time. Testing/QA took about 2 weeks of time.

We work hard on the development of the new products and on bringing the easiest to use, most capable products to market that we can. Right now, we are about to release HoneyPoint Security Server Console 3.00 and then a whole new architecture for the HoneyPoints/HornetPoints themselves. That's a lot for us and keeps our engineers and technical team hopping (or buzzing) as the case may be.

What are the major news in this release?

In the new Personal Edition we changed the interface to make it easier to use, added in the "defensive fuzzing" techniques of HornetPoints (Patent-Pending) and brought the flexibility of plugins to the product. That means that in addition to detecting scans, probes and attacks, you can also allow HornetPoints to try and defend themselves by attempting to crash the offending malware or tool that is doing the probing and you can use the plugins to automate a variety of responses from custom alerting/SEIM integration to updating other security controls or modifying the security posture of your system that is under attack.

Pretty cool stuff that our Security Server product had that we wanted to bring to the independent host product. There's a lot more to come as well. We are working on plans for more updates and capabilities for Personal Edition, even as I write this.

MicroSolved has sponsored and contributed to various open source initiatives and working groups. What projects do you support and why?

For a variety of reasons, I am not going to mention them by name. We do a lot of vulnerability research and much of that is working with a variety of open source projects. We enjoy fantastic relationships with the OSS developers and we contribute to helping many of them make their products more secure on an ongoing basis.

We consider it as a part of training new engineers and doing research on new tools, QA on tool updates and other integrated work on the business. Instead of doing those things with no outcome, we often use OSS projects as the basis for the work and then share our findings, new security vulnerabilities and other results with the project leaders. That way everyone wins! We also have a large set of tools that we contribute to community. Our web site is currently being revamped to feature them more prominently, but we have a number of free software tools that we give away when you attend our events or speaking engagements.

We also maintain the stateofsecurity.com blog, the @honeypoint Twitter feed of ongoing attack sources in real time and publish our "State of the Threat" presentations that we have been giving ongoing for more than five years.

The why is easy. The community has given so much to us over the last nearly 20 years we have been in business that we just continually strive to give back!

What are your future plans?

You will see more HoneyPoint stuff from us and more work on identifying emerging threats. You can count on us to keep looking for new ways to fight the insider threat and to help clients and members of the tribe make more rational choices about security, risk and compliance.

You can read Brent's Twitter stream at http://www.twitter.com/lbhuston

---

You can read HoneyPoint's Twitter stream at http://www.twitter.com/HoneyPoint