

Gadi Evron

Security Strategist

Email: ge@linuxbox.org

Phone: +1.415.534.0201 (US)

For my Israeli number, please email me.

Summary

I am looking for a management position in the information security industry where I can focus on building an understanding of current and future technical security issues into a cohesive security strategy. My technical knowledge of internet security, infrastructure, fraud and cyber crime risks to business and government on-line is exceptionally deep and I have a great ability to communicate these risks to decision makers.

My goal is to find a position where I can contribute technically and make a difference strategically. I believe that to be truly relevant in today's security environment it requires the use of my global contacts to help build solutions that move beyond the barriers of one given network, company, country, etc.

My strength is bringing together technically diverse people in a way that fosters cooperation to build solutions to larger problems. I am great working within the crisis, but will maintain the longer vision of once through the crisis how do we build systems and partnerships that will prevent those issues from becoming a crisis in the future.

Career highlights

- I was the first in the security industry to raise awareness of various threats, such as botnets, fastflux and DNS Amplification Attacks.
- In 2004 I chaired the world's first task force for fighting phishing and online scams
- Following the incident, I wrote the official post-mortem analysis and recommendations on the 2007 attacks against Estonia ("The First Internet War")
- During the emergencies of Hurricanes Katrina and Rita I coordinated the online response to scams taking advantage of victims, together with SANS ISC and US-CERT (DHS)
- On various occasions I facilitated global incident response for internet infrastructure incidents and cyber crime attacks
- I organize global security coordination between registrars, ISPs, law enforcement, security researchers, academics and policy makers

Publication highlights

- Working paper: With Rosanna Guadagno and Robert Cialdini, "What about Estonia? A Social Psychological Analysis of the First Internet War."
- "Battling botnets and online mobs: Estonia's defense efforts during the internet war," Georgetown Journal of International Affairs, Winter/Spring 2008, Volume IX, number 1
- Wrote chapters and tech-edited "Open Source Fuzzing Tools." Syngress, 2007
- Wrote a chapter in "Botnets: The Killer Web App," Syngress, 2007
- With Noam Rathaus and Kfir Damari, "Web server botnets and hosting farms as attack platforms." Virus Bulletin, 2007
- "Fuzzing: It Can Be Good for Finding Evil," Dr. Dobbs, 2007
- With Alan Solomon, "The world of botnets," Virus Bulletin, 2006
- With Randal Vaughn, "DNS Amplification Attacks," publicly released to mitigate attacks

Experience

Self Employed, Security Strategist

(2008 – Present)

I contract with different companies performing various functions:

- Information security, internet fraud and cyber crime consulting
- Design security architecture
- Consult Venture Capital companies and funds (VCs) on new ventures
- Trend-building and formulating long-term business strategy
- Improving communication between R&D and marketing for PR purposes

Afilias Global Registry Systems, Security Architect – a client I can disclose.

(November 2007 – May 2008)

I worked on several projects, but my overall goal was to build a new information security culture within the company that crossed all departments to get ahead of the issues that the company was experiencing. Among those projects:

- Design a DDoS attack resistant infrastructure and response plan, which is now being implemented.
- Create wide-ranging industry and community relations, positioning Afilias as a trusted and known party
- Rid Afilias' .info registry zone from fastflux domains, which was successful
- Fought the abuse by spammers by collecting actionable intelligence and building plans for an abuse desk

While doing so, I also represented Afilias in a few conferences at which I spoke, such as the United Nations Internet Governance Forum (IGF) and the European Commission's Large Scale Attacks Policy Implications Workshop.

Zeroday Emergency Response Team, Operations Manager and Founder

(2005 - Present)

ZERT is a non-profit global incident response organization working closely with vendors such as Microsoft. We provide a quick response, giving the vendor time to find a more robust solution for zero day issues affecting their products. The position requires a lot of coordination of disparate technical resources, vendors, governments and outside enterprises. See:

<http://isotf.org/zert/>

Security Conferences, Organizer

(April 2004 - Present)

ISOI stands for Internet Security Operations and Intelligence. It is a non-profit and closed workshop for vetted and trusted individuals in government, law enforcement, industry and academia world-wide. In it sensitive subjects relating to the security of the Internet infrastructure, combating cyber crime, phishing, botnets and fraud are being discussed. The conference has produced amazing results including pinpointing future security threats to the internet, and what to do about them.

- ISOI 1 was hosted by Cisco and supported by the ISC.
<http://isotf.org/isoi.html>
- ISOI 2 was hosted by Microsoft and supported by Trend Micro.
<http://isotf.org/isoi2.html>

- ISOI 3 was hosted by ICANN, ISOC and Afilias, and supported by Sunbelt Software.
<http://isotf.org/iso3.html>
- ISOI 4 was hosted by Yahoo! and supported by various local SF-bay companies.
<http://isotf.org/iso4.html>
- ISOI 5 was hosted by the Estonian CERT and supported by Norman.
<http://isotf.org/iso5.html>
- ISOI 6 was hosted by the University of Texas, Dallas, and supported by Baylor University.
<http://isotf.org/iso6.html>
- ISOI 7 will be hosted by the Websense and Eset, and supported by Facebook and SoftLayer:
<http://isotf.org/iso7.html>

I also organize TAUSEC, a monthly professional security forum at the Tel Aviv University.

Beyond Security, Security Evangelist

(2006 - 2008)

Working under the title of "Security Evangelist", in this position I fulfilled the duties of the in-between guy. On the one hand I was technical and helped design the company's products and on the other, business development. More specifically:

- I supervised and helped design two software development projects (securiteam.com web portal and the beSTORM fuzzer, a software security black box testing suite)
- Acted as editor-in-chief for SecuriTeam, then the second biggest security portal online
- Created a successful blogging site for SecuriTeam with 15,000 unique readers a month (started with 80)
- Worked closely with the marketing department as I opened new high-level sales channels
- I managed the beSIRT incident response team and formed outside relations and ties
- Wrote research papers and articles (for example, published in Virus Bulletin and developer.com)
- Spoke for the company in the press, quoted in hundreds of articles
- Represented the company in conferences, at which I spoke (Defcon, BlackHat, CSI, CISO Summit, RSA, CCC, etc.)

My duties as "evangelist" were in building a brand and creating favorable industry trends. And whether outside or inside the company, oil the communication and make things happen. Another side to this was translating business and technical people to each other.

This was supposed to be a temporary and task-specific job, for a period of two months. I stayed for two years.

Tehila, the Israeli Government ISP and eGovernment project, Information Security Manager (CISO)

(2004 - 2006)

Tehila is a department under the Israeli Ministry of Finance (which for historical reasons is in charge of IT for the government). Tehila provides the entire government with Internet service, hosting, eCommerce, etc. It is also the eGovernment (online government) project running all information, eCommerce and online forms sites. It also manages the certificate authority which will eventually integrate PKI in passports and identification cards, etc.

"You don't need your firewalls! Gadi is Israel's firewall."

-- Itzik (Isaac) Cohen, "Computers czar", Senior Deputy to the Accountant General, Israel's Ministry of Finance, at the government's CIO conference, 2005.

My responsibilities and successes:

- I developed the organization's and the government's incident response capabilities
- Established bilateral relations with foreign governments and private industry
- Represented the government in professional conferences and in the press
- Managed standardization and compliance requirements
- Designed and directed security architecture
- Helped design log management and patch management systems
- Performed penetration testing and tested new products
- Deployed IDS, Firewall and WAF systems
- Spoke for the government in the press and at conferences such as CISO Summit

Tehila, the Israeli Government ISP and eGovernment project, Israeli Government CERT manager

(2005 - 2006)

In this position we formed the Israeli Government CERT.

My responsibilities and successes:

- I was directly responsible for establishing trust relationship with other government organizations, NGOs and private industry
- Established bilateral relations with foreign governments
- We facilitated information sharing and coordinated government-wide and country-wide incident response
- We created a centralized trusted location for people having abuse and security issues in Israel to go to, and the local relationships to back that responsibility
- I spearheaded the creation of a working group to coordinate security efforts between Israeli ISPs (and other relevant organizations)
- Wrote briefings and participated in parliamentary discussions
- Spoke for the government in the press and at conferences

Self Employed, Security Consultant

(2004 - 2004)

During this year I worked with two organizations:

- Aladdin Knowledge Systems, where I briefly managed a research team in charge of responding to new virus threats
- The Israeli Central Bureau of Statistics, where I consulted on corporate security, virus protection, security strategy and compliance

IDF, Military Intelligence, Security Research and Management Positions

(2000 - 2003)

During my service in the Israeli Military I held several positions, the first of which was a technical one centered on network security. The following positions were as team leader, boot-strapping new research and analysis projects

References will be provided upon request.