New York Metro Joint Computer Security Conference

William Hugh Murray

whmurray@sprynet.com

705 Weed StreetNew Canaan, CT 06840

1-203-966-4769

1-203-326-1266 Mobile/SMS

http://whmurray.blogspot.com/

- CVEs
- Breaches
- IOCs
- Extortion payments
- Bait e-mail messages
- Hostile or corrupt URLs
- Espionage (leakage of intellectual property)
- Point of Sale compromises
- Wholesale and retail fraud
- Patches
- *et cetera, et alter*

Attack Surface

- Devices (desktops, servers, mobiles)
- Appliances ("things")
- VPN services, Remote Desktops
- USB ports
- Users
- Privileged users
- Credentials
- Operating Systems
- Gratuitous code
- Content Managers (e.g., WordPress, plug-ins
- Database Managers
- Other services
- Common Applications (word processors, spread sheets, browsers, browser extensions e-mail clients)
- *Et cetera, et alter*

Minimize the Attack Surface

- Install only what you really need
- Remove Unused or rarely used applications or services
- Prefer purpose-built apps to general and flexible facilities (e.g., browsers, spread-sheets, word processors, content managers, operating systems)
- Hide applications, systems, and services behind firewalls and end-to-end application layer encryption
- Isolate e-mail and browsing

Minimize the Attack Surface

- Employee restrictive access control (i.e., least privilege, "white-list") at all layers
- Consider Applications as a Service (e.g. Office 365)
- Scan and patch only what is left (i.e., that which can be seen by potentially hostile processes)
- Other (e.g., Mobile-based Strong Authentication, Privileged Access Management (PAM),Secure Configuration Management (SCM), Multi-party Controls, Document Management Systems, Replace passwords with asymmetric key cryptography based challenge response)