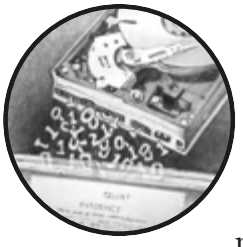
0

OGÓLNY ZARYS INFORMATYKI ŚLEDCZEJ



Szkic historycznego tła rozwoju działu informatyki, jakim jest informatyka śledcza, pomaga wyjaśnić, w jaki sposób zmieniała się ona na przestrzeni lat. Dodatkowo ułatwia uchwycenie kontekstu niektórych problemów i wyzwań, przed jakimi stają specjaliści zawodowo związani z tą branżą.

Historia informatyki śledczej

W tej części omawiam rozwój nowoczesnej informatyki śledczej jako działu nauk informatycznych.

Koniec wieku XX

Historia informatyki śledczej jest bardzo krótka w porównaniu z czasem istnienia większości dziedzin i działów nauki. Najwcześniejsze prace dochodzeniowo-śledcze związane z komputerami przypadały na lata osiemdziesiąte, kiedy eksperci byli prawie wyłącznie pracownikami organów ścigania lub organizacji wojskowych. W tamtym

czasie nastąpił wzrost liczby komputerów domowych i serwisów BBS dostępnych przez połączenia wdzwaniane. Zapoczątkowało to zainteresowanie informatyką śledczą w społeczności pracowników organów ścigania. W 1984 roku FBI opracowało pionierski program do analizy dowodów cyfrowych. Ponadto wzrost nadużyć i ataków internetowych doprowadził do utworzenia w 1988 roku Computer Emergency Response Team (CERT) – zespołu reagowania na incydenty w sieci Internet. CERT został utworzony przez agencję DARPA (Defense Advanced Research Projects Agency) na Uniwersytecie Carnegie Mellon w Pittsburgu i do dzisiaj jest z nim związany.

W latach dziewięćdziesiątych nastąpił znaczny wzrost dostępu do Internetu, a komputery osobiste w domu były już codziennością. W tym czasie informatyka śledcza stała się główną problematyką wśród organów ścigania. W 1993 roku FBI zorganizowało pierwszą z wielu międzynarodowych konferencji dla stróżów prawa, poświęconych dowodom w postaci elektronicznej. W 1995 roku powstała IOCE (International Organization of Computer Evidence), która rozpoczęła opracowywanie zaleceń dotyczących standardów postępowania w cyfrowym śledztwie. Pojęcie „przestępczości komputerowej" stało się rzeczywistością nie tylko w Stanach Zjednoczonych, lecz także na arenie międzynarodowej. W 1999 roku Association of Chief Police Officers (ACPO) opracowało przewodnik dobrych praktyk dla brytyjskich funkcjonariuszy organów ścigania, którzy zajmowali się dowodami opartymi na technologiach komputerowych. Pod koniec lat dziewięćdziesiątych powstało pierwsze oprogramowanie o otwartym kodzie źródłowym, służące informatykom śledczym. Był nim The Coroner's Toolkit stworzony przez Dana Farmera i Wietsego Venema.

2000–2010

Po przełomie tysiącleci wiele czynników zwiększyło zapotrzebowanie na informatykę śledczą. Tragedia z 11 września 2001 roku miała ogromny wpływ na to, jak świat zaczął postrzegać bezpieczeństwo i reagowanie na incydenty. Skandale księgowe dotyczące firm Enron i Arthur Andersen doprowadziły do stworzenia w Stanach Zjednoczonych ustawy Sarbanesa-Oxleya. Ma ona na celu ochronę inwestorów dzięki poprawie dokładności i wiarygodności ładu informacyjnego (oświadczeń o stanie firmy). Akt ten wymaga, aby organizacje sformułowały oficjalne procedury procesów dochodzeniowych i reagowania na incydenty, zwykle obejmujące pewne elementy informatyki śledczej lub gromadzenia cyfrowego materiału dowodowego. Wzrost znaczenia własności intelektualnej (IP) miał również wpływ na organizacje prywatne. Oszustwa internetowe, wyłudzanie informacji i inne naruszenia własności intelektualnej i nazw zastrzeżonych spowodowały dalszy wzrost zapotrzebowania na śledztwa i gromadzenie dowodów. Udostępnianie plików w sieciach peer-to-peer (począwszy od Napstera) wraz z pojawieniem się cyfrowego prawa autorskiego w postaci ustawy Digital Millennium Copyright Act (DMCA) doprowadziło do wzrostu zapotrzebowania na dochodzenia dotyczące naruszeń cyfrowego prawa autorskiego.

Od 2000 roku społeczność zajmująca się informatyką śledczą poczyniła ogromne postępy, nadając tej dziedzinie postać dyscypliny naukowej. Konferencja DFRWS w 2001 roku przyniosła ważne definicje i wyzwania stające przed społecznością śledczych. Zdefiniowano wtedy informatykę śledczą jako:

> Wykorzystanie naukowo udowodnionych i potwierdzonych metod zabezpieczania, gromadzenia, weryfikacji, identyfikacji, analizy, interpretacji, dokumentacji

i prezentacji cyfrowego materiału dowodowego, pozyskanego ze źródeł elektronicznych, w celu umożliwienia lub ułatwienia rekonstrukcji działań określanych jako przestępcze lub pomocy w przewidywaniu nielegalnych czynów, będących zakłóceniami zaplanowanych czynności[1].

Podczas gdy społeczność śledczych określała cele i zakres działań budujących naukowe podstawy tej dziedziny, opracowano również standardy postępowania, wytyczne i najlepsze praktyki w zakresie stosowanych procedur. Grupa badawcza Scientific Working Group on Digital Evidence (SWGDE) określiła definicje i standardy, w tym wymogi standardowych procedur operacyjnych (Standard Operating Procedures – SOP) dla organów ścigania.

We Francji podczas konferencji IOCE 2000 pracowano nad sformalizowaniem procedur działania techników-funkcjonariuszy dzięki wytycznym i listom kontrolnym. 13. INTERPOL Forensic Science Symposium, również we Francji, wyznaczyło wymagania stawiane grupom zaangażowanym w informatykę śledczą i określiło obszerny zestaw norm i zasad dla władz i organów ścigania. Amerykański Departament Sprawiedliwości opublikował szczegółowy przewodnik szybkiego reagowania dla stróżów prawa (US DOJ *Electronic Crime Scene Investigation: A Guide for First Responders*). W ramach projektu NIST's Computer Forensics Tool Testing (CFTT) napisano natomiast specyfikację narzędzia do tworzenia obrazu dysku (*Disk Imaging Tool Specification*).

W ciągu tego dziesięciolecia ukazało się kilka recenzowanych czasopism naukowych mających na celu prezentowanie stale rosnącego zasobu wiedzy. *International Journal of Digital Evidence* (IJDE) powstał w 2002 roku (i zakończył działalność w 2007 r.), a *Digital Investigation: The International Journal of Digital Forensics* & *Incident Response* został utworzony w 2004 roku.

2010–obecnie

W latach po 2010 roku wiele wydarzeń zmieniło podejście do badania i gromadzenia dowodów z cyberataków i naruszeń bezpieczeństwa danych.

Serwis WikiLeaks (*http://www.wikileaks.org/*) zaczął publikować materiały, które wyciekły z amerykańskiego wojska, w tym filmy i depesze dyplomatyczne. Anonimowi zyskali rozgłos w związku z rozproszonymi atakami typu DoS (Denial of Service) i innymi działaniami haktywistów. LulzSec naruszył bezpieczeństwo i ujawnił dane z HBGary Federal i innych firm.

Badanie szkodliwego oprogramowania Advanced Persistent Threat (APT) stało się głównym zagadnieniem w branży. Opinia publiczna poznała zakres rządowych technik wywiadowczych z zastosowaniem złośliwego oprogramowania, stosowanych zarówno wobec innych rządów, jak i sektora prywatnego. Został odkryty robak Stuxnet, atakujący systemy SCADA. Szczególnym przypadkiem jego działania było zakłócenie systemów kontrolnych irańskiego programu jądrowego. Mandiant opublikował swoje dochodzenie w sprawie APT1, jednostki do walki cybernetycznej w chińskiej armii. Edward Snowden ujawnił obszerne repozytorium dokumentów, odsłaniające zakres hackowania przez NSA. Publikacja danych włoskiej firmy HackingTeam ujawniła, że z profesjonalnego rynku exploitów korzystają rządy, organy ścigania i firmy sektora prywatnego.

[1] Gary Palmer, „A Roadmap for Digital Forensic Research". Digital Forensics Research Workshop (DFRWS), 2001. Technical report DTR-T0010-01, Utica, New York.