I trend della sicurezza 2015

Walter Narisoni

Sales Engineer Manager

SOPHOS

La sicurezza informatica nel 2015

- Mitigazione degli exploit
- Attacchi all' «Internet of Things»
- Cifratura diventa uno standard
- Aumento difetti su SW di uso comune
- Problemi nel panorama legislativo
- I sistemi di mobile payment
- Aumento dei servizi di attacco per mobile
- ICS/SCADA e la sicurezza
- Nuove funzionalità, nuovi vettori di attacco

Mitigazione degli exploit

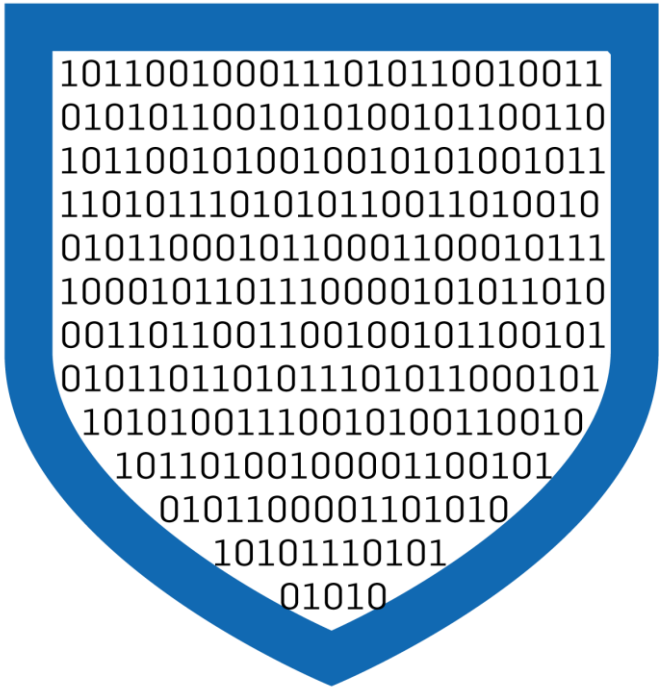
- Oggi le infezioni arrivano via web
- Microsoft ha investito nella mitigazione degli exploit
- Gli exploit diventano più cari e vengono utilizzati per attacchi mirati
- Sta tornando il social engineering
- Aumento degli attacchi verso piattaforme non Microsoft
- Fondamentale aumentare la sicurezza degli ambienti non Microsoft

Attacchi all’ «Internet of Things»

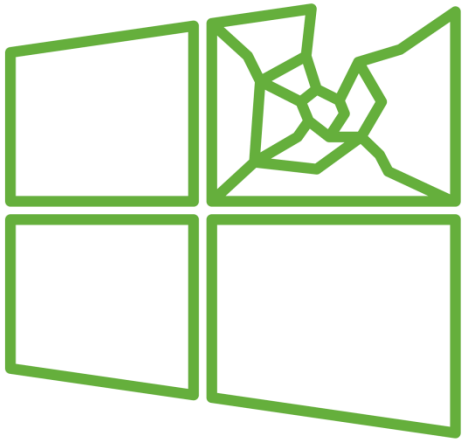
- Bassa sicurezza nell’ «Internet of Things»
- Possibilità di nuove tipologie di attacchi
- Gli attacker non hanno ancora trovato come lucrare
- Alcuni vendor non dispongono dell’infrastruttura per la distribuzione degli aggiornamenti

Cifratura diventa uno standard

- Cifratura sta diventando un default per tutte le piattaforme
- Molte applicazioni utilizzano SSL, ma senza certificate pinning
- Cifratura a scopo promozionale
- Forze dell'ordine e servizi segreti sono contro la cifratura
- Maggior traffico cifrato vuole dire che gli apparati sulla rete non riescono ad analizzarlo



Aumento difetti su SW di uso comune



- Molti computer contengono frammenti di codice non sicuro
- OpenSSL con poche risorse per il controllo del codice
- Tutti hanno sistemi per distribuire le patch su Microsoft ma gli altri S.O.?
- Dopo mesi vi sono ancora prodotti vulnerabili a Heartbleed
- I cybercriminali oggi sono interessati a SW e S.O. meno famosi

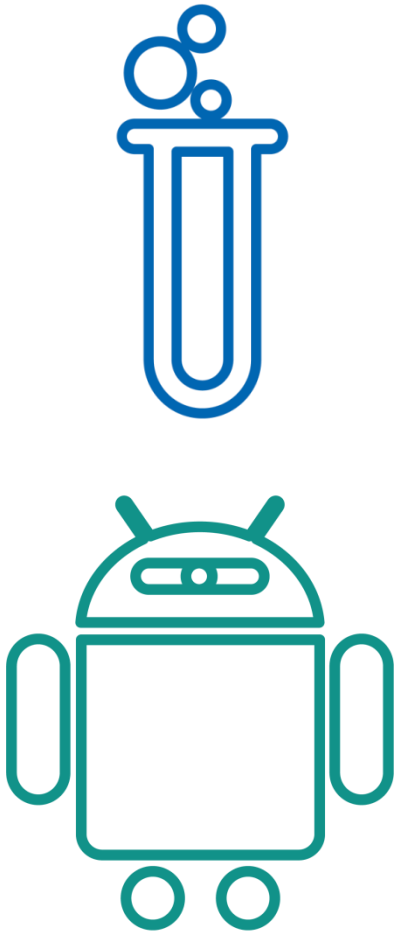
Problemi nel panorama legislativo

- L'Unine Europea introdurrà nuovi standard per la protezione dei dati (a partire dal 2016)
- Multe che possono arrivare a 100 milioni di euro o il 5% del proprio fatturato annuale
- Implementazione delle leggi a livello nazionale, ma il cybercrime è un problema internazionale

I sistemi di mobile payment

- I criminali studieranno questi sistemi alla ricerca di difetti
- Le attuali strutture sono più sicure dei metodi tradizionali (carta di credito)
- Passo avanti contro la clonazione delle carte di credito
- I criminali continueranno ad attaccare i metodi tradizionali
- Da tenere d’occhio le vulnerabilità dei nuovi strumenti

Aumento dei servizi di attacco per mobile

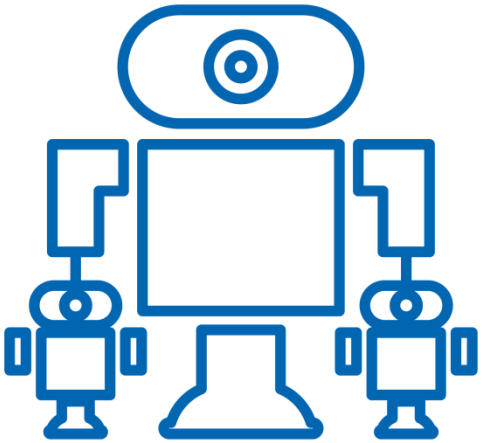


- Kit di attacco hanno esteso la propria applicazione alle piattaforme mobili
- Maggior parte del malware è rivolto ad Android
- Fortunatamente gli aggiornamenti automatici stanno diventando uno standard
- Nel futuro ci sarà sempre più attenzione da parte dei cybercriminali a questo tipo di piattaforma

ICS/SCADA e la sicurezza

- Divario tra ICS/SCADA e la sicurezza nel mondo reale aumenta
- Unica strategia mantenerle isolate in reti di tipo «air gap»
- Purtroppo alcuni di questi sono collegati a reti esterne
- Basta utilizzare tool come Shodan per individuarne parecchi
- Da attacchi a scopo di lucro ad attacchi di differente tipo

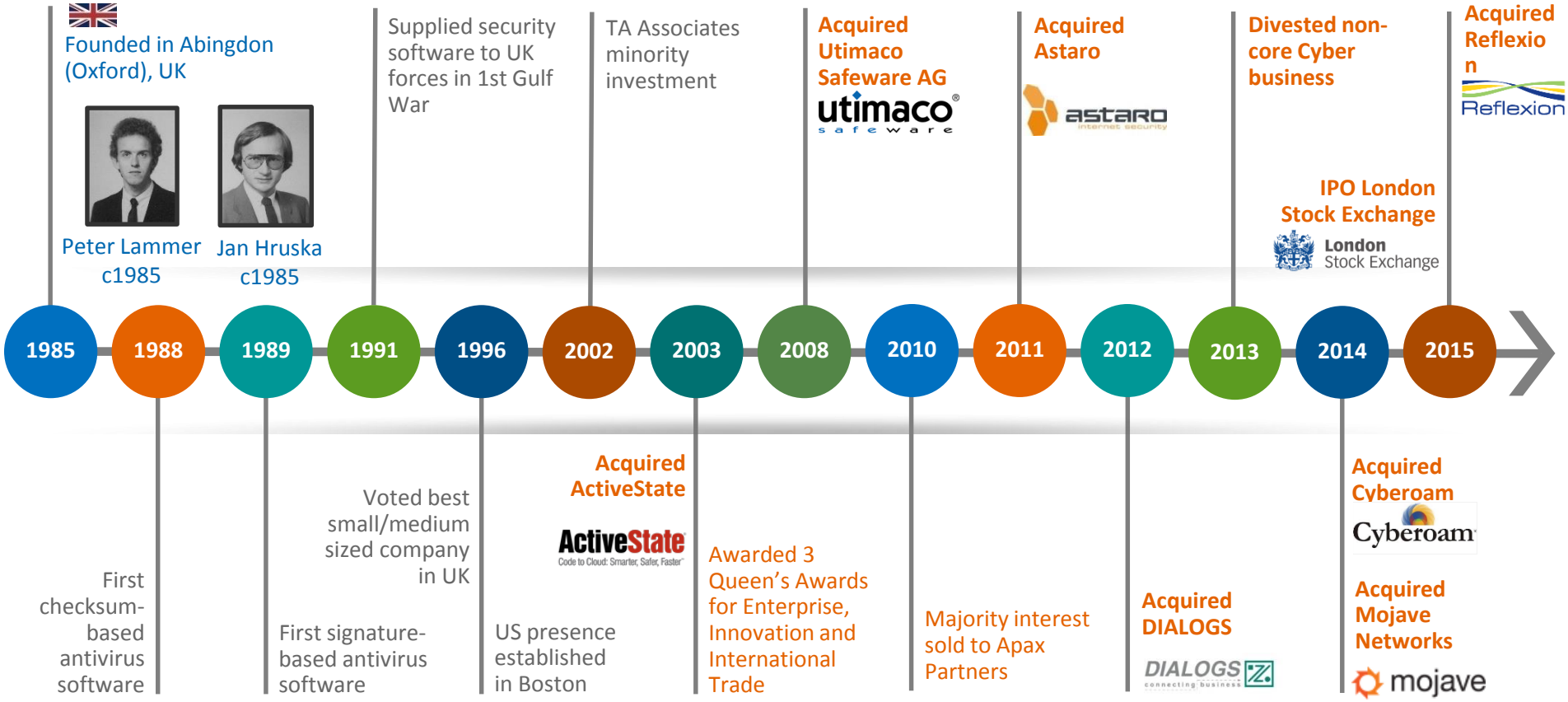
Nuove funzionalità, nuovi vettori di attacco



- Nuove piattaforme e protocolli (http 2.0 e IPv6) nuovi attacchi
- IPv6 implementa alcuni vecchi difetti di IPv4 (possibilità di fare attacchi di tipo man-in-the-middle)
- UEFI offre a rootkit e bot nuove funzionalità
- Sembra che siamo destinati a rifare parecchi degli errori che abbiamo fatto nel passato

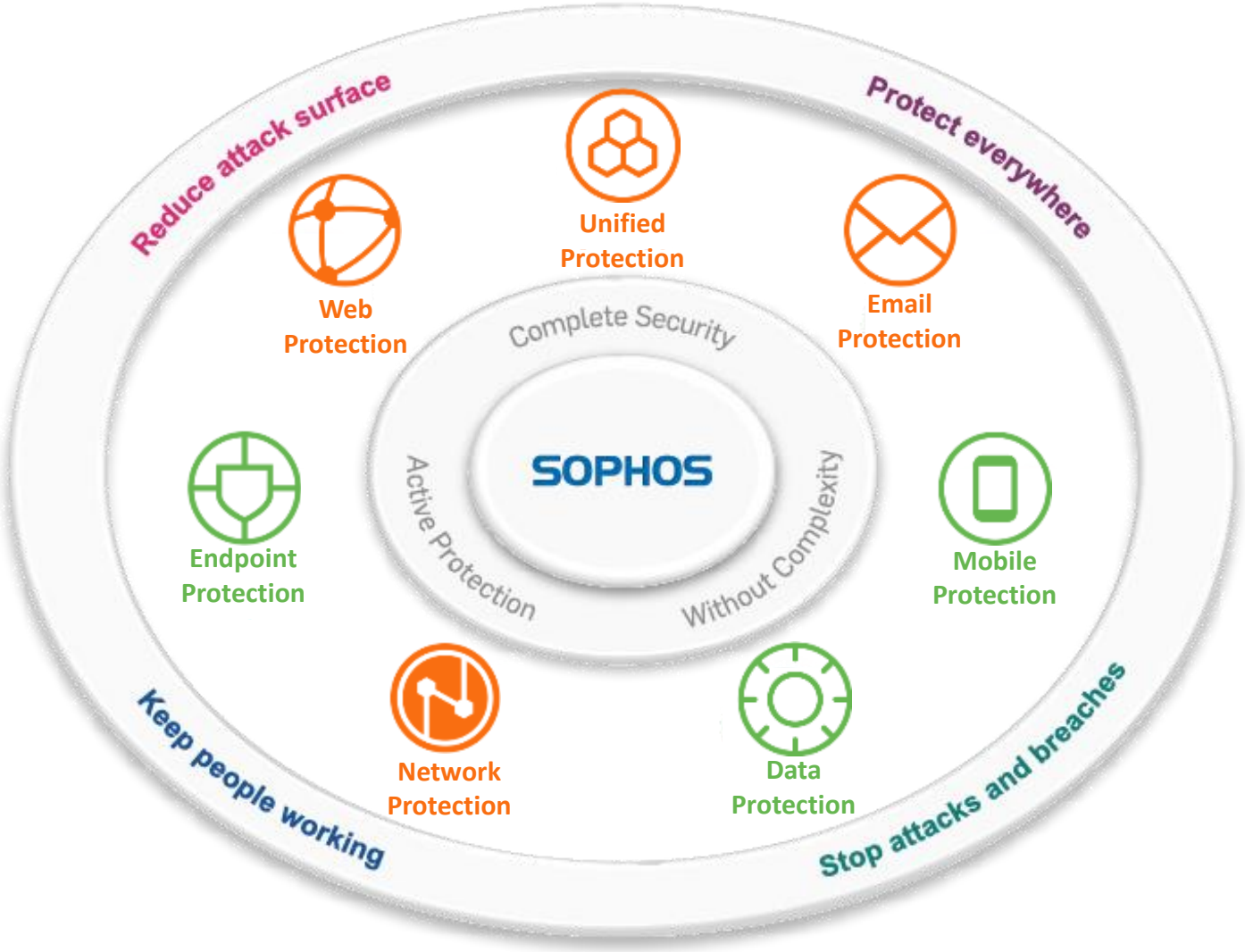
Sophos History

Evolution to complete security



Complete Security

Protecting every part of your business



SOPHOS