



Cosa fare PRIMA di cadere vittima di un attacco:

la sicurezza informatica per le nuove minacce



Sommario

I rischi alla sicurezza sono più elevati che mai.....	3
L'utente è sempre l'anello più debole	4
Quanto costa realmente un attacco informatico?	4
Clienti e server.....	4
Le strategie di sicurezza non mirate portano solo a costi eccessivi.....	5
Gestione delle patch: un problema non ancora risolto	5
Altri problemi segnalati dai nostri clienti.....	6
Il futuro? Malware come armi cibernetiche	6
Le strategie di sicurezza mirate portano al successo IT	6
Il valore del CIS	7
Un nuovo livello di sicurezza con i primi 5 CSC.....	7
Le nostre soluzioni di difesa approfondita.....	8
Vi possiamo aiutare a valutare i risultati.	8
Conclusione.....	9

Questo documento è fornito unicamente a scopo informativo. Non rappresenta alcuna garanzia. Questo documento contiene informazioni che sono riservate e/o di proprietà di Ivanti, Inc. e delle sue società affiliate (collettivamente "Ivanti") e non possono essere divulgate senza la preventiva autorizzazione scritta di Ivanti.

Ivanti si riserva il diritto di apportare modifiche a questo documento o a specifiche e descrizioni di prodotti correlate, in qualsiasi momento e senza preavviso. Ivanti non fornisce alcuna garanzia sull'uso del presente documento e non si assume alcuna responsabilità per eventuali errori in esso contenuti, né si impegna ad aggiornare le informazioni in esso contenute. Per informazioni aggiornate sui prodotti,

visitate www.Ivanti.com.

Introduzione

Nel 2016, nei soli Stati Uniti sono state dichiarate più di 500 violazioni di dati, quasi il doppio rispetto all'anno precedente.¹ Nel febbraio 2017, da uno studio condotto dalla Opinium emerge che tra i decision maker IT che hanno partecipato alla ricerca negli USA e in Europa, il 78% ha subito almeno un attacco ransomware nella propria organizzazione negli ultimi 12 mesi. Shadow Brokers, il gruppo di hacking che ha portato alla luce la vulnerabilità sfruttata da WannaCry, ha promesso di rivelare altri casi simili su base regolare, e sta già mantenendo tale promessa. È già stato reso pubblico il primo pagamento di un riscatto da un milione di dollari.² NotPetya ci ha fornito un assaggio delle armi malware del futuro. E poi c'è stato Equifax...

Come fermare questo treno in corsa? Senza una strategia di sicurezza mirata, l'utilizzo esteso di dispositivi mobili comporta costi elevati ed è difficile da gestire. I team IT dedicano troppo tempo alla gestione di tali dispositivi. Inoltre, a causa della forte carenza di specialisti della cybersicurezza, le aziende si trovano obbligate a ottimizzare il personale addetto alla sicurezza informatica. È chiaro, quindi, che conviene orientarsi su una strategia basata su soluzioni tecnologiche complete in grado di semplificare la gestione, e concentrarsi sugli aspetti di base della sicurezza per difendersi contro attacchi reali.

Quando il 93% delle violazioni di dati sono tali da compromettere le organizzazioni in pochi minuti,³ non ci si può permettere decisioni errate in fatto di sicurezza dell'organizzazione.

I rischi alla sicurezza sono più elevati che mai

Tutte le principali minacce informatiche sono in aumento.⁴ È un fatto che non sorprende, ma perché siamo arrivati a tale situazione?



Una delle ragioni principali sta nella facilità con cui è ormai possibile sferrare attacchi informatici. Anche gli hacker meno esperti possono procurarsi exploit kit che ne semplificano la programmazione. Si tratta di toolkit con codice precompilato che non richiedono conoscenze particolari. Spesso una semplice interfaccia Web consente a chi dispone di una licenza di accedere e visualizzare vittime attive e statistiche. Questi kit possono addirittura includere un periodo di supporto e aggiornamenti, proprio come i normali programmi software in commercio.

Un altro fattore è l'ampia disponibilità di strumenti sofisticati originariamente destinati allo spionaggio informatico e alla guerra cibernetica.

Il ransomware, ad esempio, si è evoluto da una semplice tecnica di hacking fino a diventare malware di dimensioni enterprise creato con strumenti sottratti alla U.S. National Security Agency (NSA), in grado di tenere in ostaggio i computer e bloccare interi sistemi. Considerando poi il fatto che quasi il 40% di tutto lo spam inviato nel 2016 conteneva ransomware,⁵ è solo questione di tempo prima che un utente in buona fede faccia clic su un link che non dovrebbe toccare e comprometta l'intera organizzazione.

Stando a una ricerca condotta da IBM X-Force, un dirigente su due ha sofferto un attacco ransomware a

lavoro. Si tratta potenzialmente della metà dei dirigenti della vostra organizzazione.⁶

L'utente è sempre l'anello più debole

Verizon Data Breach Investigations Report (DBIR) è uno dei più rispettati report annuali nel settore della sicurezza. Ogni anno il team Verizon Research, Investigations, Solutions and Knowledge (RISK), una delle maggiori realtà investigative in campo IT al mondo, condivide informazioni approfondite sullo stato della sicurezza informatica e sulle maggiori tendenze.

Nel 2017, questo team ha evidenziato che il phishing è usato in più del 90% degli incidenti di sicurezza e violazioni.⁷

E con frequenza ugualmente allarmante, gli utenti con i loro diversi dispositivi cadono vittima di ransomware ed altri attacchi malware diretti proprio agli utenti. Secondo Verizon, nel 2016 è stato aperto il 30% dei messaggi di phishing, con un aumento del 23% rispetto all'anno precedente. Nel 12% di tali casi, gli utenti hanno fatto clic per aprire l'allegato o il link dannoso.⁸

Il report Verizon 2016 DBIR evidenzia che è in aumento la tipologia di attacco di phishing in tre fasi:

- L'utente riceve un'e-mail di phishing con un allegato dannoso o un link verso un sito Web dannoso.
- L'utente scarica un malware, con cui l'hacker può accedere a dati riservati, sottrarre credenziali di accesso per diverse applicazioni tramite key logging, o cifrare i file da tenere in ostaggio.
- Inoltre le credenziali sottratte possono essere utilizzate per attacchi futuri. Ad esempio, per accedere a siti di banking o di vendita online.

Quanto costa realmente un attacco informatico?

Secondo le stime della FBI, nel primo trimestre del 2016 i crimini informatici hanno fruttato 209 milioni di dollari, e supereranno probabilmente il miliardo di dollari entro la fine dell'anno.⁹ Da allora, la situazione non ha fatto che peggiorare. Ed è stata pubblicata la notizia del primo pagamento di riscatto da un milione di dollari.¹⁰

Ma malware e ransomware vanno ben oltre il semplice guadagno economico.

WannaCry, nonostante un impatto economico tutto sommato esiguo (circa 135 mila dollari al 28 giugno 2017), ha invece riscosso enorme successo in termini di diffusione: in un solo giorno sono infatti stati infettati più di 230 mila computer in oltre 150 paesi. Per le organizzazioni, il costo va ben oltre il pagamento del riscatto. Non vi è alcuna garanzia che, una volta pagato il riscatto, i dati vengano recuperati. Inoltre, i veri danni

sono di altra natura: tempo di inattività dei sistemi, dati danneggiati, perdita di produttività e complicazioni post-attacco nel normale svolgimento delle attività aziendali, investigazioni forensi e ripristino di dati e sistemi. Per non parlare di lesione della reputazione presso clienti, partner e catena di fornitura qualora venissero evidenziate lacune di compliance.

FedEx, l'azienda farmaceutica Merck e il gigante delle spedizioni Maersk sono esempi di grande rilievo. Tutti e tre sono stati colpiti da NotPetya, e hanno ammesso di subirne ancora le conseguenze a distanza di settimane e mesi. In FedEx, i sistemi sarebbero stati completamente ripristinati entro la fine di settembre, tre mesi dopo l'attacco, con un costo di 300 milioni di dollari.¹¹ Anche Maersk ha calcolato cifre simili,¹² mentre per Merck i costi sono stimati tra i 200 e i 300 milioni di dollari.¹³

Clienti e server

Come è possibile che anche le aziende più grandi, che sicuramente dispongono di potenti strumenti di sicurezza, cadono vittima di tali attacchi?

Innanzitutto, molti strumenti non proteggono le risorse più vulnerabili.

Al sondaggio 2016 Global Business Technographics® Security Survey di Forrester hanno partecipato 192 decision-maker in ambito di sicurezza delle reti, le cui aziende (con oltre 1000 dipendenti) hanno subito violazioni alla sicurezza dall'esterno negli ultimi 12 mesi. È stato chiesto ai partecipanti quali aspetti dell'infrastruttura sono stati presi di mira dall'attacco esterno. Le risposte evidenziano che occorre focalizzarsi su client e server nella rete, e non sul perimetro dell'ambiente IT.

Quale delle seguenti aree è stata colpita dall'attacco?

Sondaggio Forrester's Global Business Technographics Security, 2016



Le strategie di sicurezza non mirate portano solo a costi eccessivi

Sfortunatamente, anche se si dispone degli strumenti giusti per proteggersi da questo tipo di attacchi, si tratta solo di alcuni dei tanti che occorre configurare e gestire ogni giorno.

Firewall di rete e di applicazioni Web, sistemi di prevenzione delle intrusioni, analisi delle vulnerabilità... La diffusione incontrollata dei dispositivi è costosa, e i team IT dedicano troppo tempo alla loro gestione. Tempo prezioso che viene sottratto ad altre attività di sicurezza il cui obiettivo è la protezione e la risposta alle minacce reali a cui è esposto l'ambiente.

Gestione delle patch: un problema non ancora risolto

Anche se si dispone degli strumenti giusti, spesso questi non sono ottimizzati.

La gestione delle patch, ad esempio, è un problema ancora da risolvere. WannaCry e NotPetya si sono diffusi rapidamente utilizzando una combinazione di exploit sottratti all'NSA e di punti deboli comuni nei software Windows, nonostante esistessero già le relative patch.

- **Il software è vulnerabile di natura.** È composta da centinaia di migliaia di righe di codice, scritte da normali esseri umani. Ed errare è umano. Nessuno scrive codice assolutamente privo di errori e immune a potenziali attacchi.
- **Più il software è datato, più vulnerabilità vengono esposte.** A noi di Ivanti piace usare la metafora del latte andato a male. Più il latte resta lì, più invecchia. E alla fine va a male. Lo stesso vale per il software: più tempo passa, più vulnerabilità vengono portate alla luce e sfruttate.
- **Ai software legacy non vengono applicate le patch.** È vero che esistono delle eccezioni. Ad esempio, dopo l'attacco WannaCry, Microsoft ha deciso di rilasciare patch anche per i sistemi operativi precedenti non più supportati, data la diffusione della minaccia. Ma in genere non si può essere certi di poter applicare patch a software datati.

- **Ai software più nuovi non vengono applicate le patch correttamente.** Prima dell'attacco WannaCry erano già disponibili le patch necessarie per i sistemi supportati, e dopo l'attacco sono state rilasciate anche per i sistemi non supportati. Eppure, nonostante l'esistenza delle patch e la recente minaccia di WannaCry, solo un mese più tardi molte organizzazioni sono comunque state colte di sorpresa da NotPetya. Forse non avevano gli strumenti necessari per applicare le patch a tutto l'ambiente. Forse a causa di risorse limitate non hanno avuto il tempo di applicarle. Qualunque sia il motivo, resta il fatto che le patch disponibili non vengono implementate come dovrebbero.
- **E infine, le patch non sono la soluzione a tutto.** Le



patch non proteggono da attacchi zero-day. È possibile che non esistano patch per alcuni sistemi datati, o che l'applicazione di una patch possa causare altri problemi nell'ambiente. Occorre quindi poter bloccare le applicazioni a cui non vengono applicate le patch, ad esempio tramite whitelist di applicazioni e con la gestione delle autorizzazioni. Indipendentemente dalla modalità o dal luogo di accesso di un utente al suo computer desktop, è fondamentale che riceva solo le app autorizzate effettivamente necessarie per il suo lavoro. All'utente non deve essere permesso introdurre app non autorizzate che potrebbero ridurre la stabilità del computer, presentare un problema di sicurezza, violare i termini delle licenze, causare tempi di inattività e aumentare i costi di gestione del computer.

Altri problemi segnalati dai nostri clienti

Il grande puzzle della sicurezza informatica ha innumerevoli pezzi. In termini semplici, tuttavia, si può riassumere la situazione così: i team IT e Sicurezza ce la mettono tutta, ma non ce la possono fare.

Le numerose singole soluzioni per specifici aspetti della sicurezza informatica non sono integrate e non forniscono un quadro completo dei rischi a cui è esposto l'ambiente. Secondo il report Cisco 2017 Annual Cybersecurity Report, il 55% dei professionisti della sicurezza utilizza soluzioni di almeno sei diversi produttori.



A questo si aggiunge la carenza di risorse specializzate nella sicurezza informatica. Senza gli specialisti e gli strumenti in grado di rilevare le situazioni critiche e comprendere perché si verificano, la fase di investigazione viene spesso saltata del tutto. Secondo lo stesso report, quasi metà degli avvisi di sicurezza non vengono sottoposti a indagine.

Immaginate il potenziale impatto di queste minacce non investigate su produttività, soddisfazione dei clienti e fiducia nell'organizzazione.

Inoltre, l'utilizzo di soluzioni e piattaforme da numerosi diversi produttori crea dei punti ciechi che possono essere sfruttati da attacchi, fa aumentare rischi e costi, e rappresenta un carico di lavoro maggiore per la governance IT e per i team già sovraccarichi.

Il futuro? Malware come armi cibernetiche

Non vi è alcun dubbio: gli hacker oggi possono avere un grande impatto sulle infrastrutture critiche nel mondo, quali ospedali e sistemi di banking, in particolare se appoggiati da sistemi software datati e vulnerabili. E sono sempre più determinati.

È uno scenario da incubo. Ma gli attacchi informatici diventano più evoluti, anche grazie ai sofisticati strumenti, originariamente destinati allo spionaggio informatico e alla

guerra cibernetica, che ora sono alla portata di qualsiasi criminale informatico.

Il ransomware WannaCry ha messo in ginocchio i computer di ospedali, istituti bancari e aziende in tutto il mondo. Nel Regno Unito, gli enti ospedalieri hanno dovuto rifiutare pazienti mentre erano alle prese con i computer tenuti in ostaggio. Anche NotPetya ha preso di mira ospedali causando l'annullamento di interventi chirurgici, e altre importanti organizzazioni come linee aeree, istituti bancari, la centrale nucleare di Chernobyl, e una grande azienda di spedizioni, che ha dovuto chiudere diversi terminali per container in numerosi porti, da Los Angeles a Mumbai.

In che modo, quindi, è possibile proteggere le organizzazioni dai pericoli di questo tipo di attacchi evoluti e di tale portata?

Le strategie di sicurezza mirate portano al successo IT

Una strategia di sicurezza di successo ha diversi aspetti. In particolare, un approccio a più livelli offre diverse opzioni di difesa per qualsiasi situazione. È importante eliminare i punti ciechi.

Difesa approfondita

- Individuare la portata del rischio
- Ridurre la superficie di attacco
- Individuare le attività dannose
- Applicare le misure necessarie
- Analizzare i dati per capire a fondo i problemi

Semplificate e automatizzate la sicurezza per migliorare i tempi di risposta

- Poiché è impossibile proteggere o proteggersi da ciò di cui si ignora l'esistenza, è fondamentale poter contare su un quadro completo di quanto accade nell'ambiente.
- Riducete la superficie di attacco: evitate che malware ed exploit possano essere eseguiti. Il team e le soluzioni di sicurezza avranno così la possibilità di stanare le minacce che riescono ad infiltrarsi nell'ambiente.
- Individuate eventuali attività dannose in seguito all'esecuzione di malware.
- Correggete e limitate i danni derivanti da attività di malware e potenziali vulnerabilità.
- E sostenete ogni sforzo con rich data sulla situazione di sicurezza e compliance.

Inoltre, sono necessari strumenti più semplici in grado di automatizzare i processi di sicurezza. L'automazione può essere di grande aiuto per alleggerire il carico delle attività di rilevamento e indagine per risorse già sovraccariche. E infine, una soluzione di mitigazione delle minacce deve essere in grado di salvaguardare e addirittura migliorare la produttività degli utenti. Infatti, è bene tener conto del fatto che gli utenti che non sono in grado di svolgere il proprio lavoro si rivolgono più spesso all'help desk o addirittura ricorrono a soluzioni di "shadow IT", introducendo elementi di rischio nell'ambiente.

Sicurezza ed esigenze degli utenti

- **Scoprite le abitudini ed esigenze degli utenti.**
- **Protegete i sistemi senza ostacolare il lavoro.**
- **Fornite servizi non invasivi con aggiornamenti e riduzione dei rischi.**
- **Aumentate la produttività con gli strumenti giusti.**



Il valore del CIS

La via migliore per passare da questa visione alla realtà è attraverso una solida struttura di sicurezza. Per ridurre i costi e migliorare la capacità di risposta, i team addetti alla sicurezza e all'IT possono unire le forze e promuovere una soluzione mirata basata su processi comuni e un set di azioni prioritarie.

Questo approccio è avvalorato da enti quali Center for Internet Security (CIS), che contribuiscono con le proprie

conoscenze e competenze a identificare, convalidare, promuovere e sostenere l'adozione di best practice in tema di sicurezza informatica. Basati su procedure elaborate dalle esperienze presso l'NSA, CIS ha definito il set di controlli Critical Security Controls, che supportano e convalidano molte delle fonti leader di linee guida per la sicurezza informatica.

Il loro obiettivo è quello di aiutarvi a determinare un punto di partenza per le vostre difese, indirizzare le risorse verso le attività che possono garantire risultati immediati ed elevato valore, e concentrarvi sui rischi specifici per la vostra realtà.

- Elenco di azioni in ordine di priorità
- Risultati immediati e di elevato valore
- Conformità normativa
- Sulla base di esperienze di attacchi reali

Framework comprovato, soluzioni da un singolo produttore in grado di rispondere alla maggior parte delle esigenze nell'intera azienda, e soluzioni specifiche per esigenze specifiche: questi sono gli ingredienti per ridurre i costi e definire una strategia efficace e approfondita.

I casi di studio e le ricerche condotte da CIS mostrano che, configurando i sistemi IT in linea con i benchmark di CIS, è possibile eliminare dall'80 al 95% delle vulnerabilità note.

Un nuovo livello di sicurezza con i primi 5 CSC

In particolare, i primi 5 Critical Security Controls (CSC) definiti d CIS permettono di gettare basi solide grazie alle quali sarà possibile migliorare radicalmente lo stato di sicurezza dell'organizzazione. Per questo le definiscono "Foundational Cyber Hygiene" (Regole di base per l'igiene informatica).

- 1. Inventario dei dispositivi autorizzati e non autorizzati**
Citando CIS,¹⁴ "Gestite attivamente (con inventario, tracciamento e correzioni) tutti i dispositivi hardware in rete, per concedere i diritti di accesso solo ai dispositivi autorizzati e negarli a quelli non autorizzati e non gestiti che vengono rilevati."
- 2. Inventario dei software autorizzati e non autorizzati**
Come sopra, ma per il software: "Gestite attivamente (con inventario, tracciamento e correzioni) tutti i software in rete, per concedere i diritti di accesso solo ai software autorizzati, e impedire l'installazione e l'esecuzione di quelli non autorizzati e non gestiti che vengono rilevati."
- 3. Configurazione sicura per hardware e software**
"Definite, implementate e gestite attivamente (con tracciamento, report e correzioni) la configurazione

di sicurezza di laptop, server e postazioni mediante la gestione rigorosa delle configurazioni. Modificate il processo di controllo per impedire che i servizi e le impostazioni vulnerabili possano essere sfruttati. In genere, infatti, le configurazioni predefinite rilasciate da produttori e rivenditori per sistemi operativi ed applicazioni sono tali da agevolarne la distribuzione e l'utilizzo, e non da potenziarne la sicurezza.”

4. Valutazione e risoluzione continua delle vulnerabilità

“Acquisite e valutate le informazioni con continuità, intervenendo ove necessario, al fine di individuare le vulnerabilità, applicare le misure necessarie e ridurre al minimo la finestra di opportunità per gli attacchi.”

5. Utilizzo controllato dei privilegi di amministratore

“L’abuso dei privilegi di amministratore è il principale mezzo sfruttato dagli attacchi per infiltrarsi e diffondersi in un’azienda.” Fornite processi e strumenti per “tracciare, controllare e impedire l’uso, l’assegnazione e la configurazione di autorizzazioni amministratore su computer, reti ed applicazioni.”

Le nostre soluzioni possono esservi di grande aiuto. Ivanti offre un portfolio completo e mirato che risponde ai 5 principali controlli e agli altri controlli CSC, allineando le iniziative dei team IT e Sicurezza per rispondere al meglio alle esigenze degli utenti in fatto di sicurezza informatica.

Le soluzioni Ivanti sono incentrate su capacità automatizzate quali discovery, gestione delle patch, controllo di applicazioni e dispositivi, gestione delle autorizzazioni di livello amministratore e configurazione della sicurezza: tutti elementi essenziali dei 5 maggiori controlli definiti da CIS. Inoltre, Ivanti aiuta i clienti a implementare con successo e facilità tali controlli, in modo conveniente e senza ostacolare la produttività degli utenti. Gli utenti non dovranno rivolgersi spesso al service desk per richiedere autorizzazioni di accesso. Né sentiranno la necessità di ricorrere a soluzioni “shadow IT” non autorizzate e non sicure. E tutte le attività aziendali verranno svolte in modo rapido e sicuro.

Vi possiamo aiutare a valutare i risultati.

La validità delle misure di difesa dipende dalle informazioni

Le nostre soluzioni di difesa approfondita

Per ogni asset business-critical nell’organizzazione, è importante confrontare i controlli di sicurezza esistenti rispetto ai Critical Security Controls definiti da CIS. Individuate esattamente eventuali controlli secondari già in essere e quelli di cui invece non disponete. Quindi, sulla base dei punti ciechi individuati e di specifici rischi e problematiche per la

Gestione delle patch e delle vulnerabilità	Controllo delle app e gestione delle autorizzazioni
Proteggete e applicate le patch ai sistemi operativi e alle app di terze parti.	Impedite l’esecuzione di altre app e limitate le autorizzazioni.
Sicurezza degli endpoint	Gestione della sicurezza dei programmi
Aggiungete capacità antimalware e antivirus, controllo dei dispositivi e criteri globali per tutti i dispositivi.	Associate alle capacità di sicurezza flussi di lavoro e processi per la gestione degli asset, per un ciclo di vita sicuro a 360°.



vostra azienda, implementate subito i 5 controlli principali e sviluppate un piano strategico per implementare gli altri.



sull’effettivo stato dell’ambiente. Con Ivanti Xtraction la reportistica è semplificata grazie a semplici caselle da spuntare, con dati on-demand e la possibilità di creare facilmente nuovi dashboard e report con cui trasmettere i dati pertinenti a dirigenti, manager e responsabili di applicazioni e line-of-business (LOB).

Grazie ai connettori preconfigurati disponibili per quasi tutti gli strumenti presenti nelle aziende (per service desk, monitoraggio e gestione degli asset IT, sistemi telefonici, ecc.) non occorre ricorrere alla programmazione, a esperti

di business intelligence o a fogli di calcolo, né a data silos. Inoltre, Xtraction può essere personalizzato per ulteriori possibilità di connessione. Tutti gli interessati possono quindi prendere visione dei dati relativi all'intera azienda nel loro contesto, estraendo dall'enorme mole di dati proprio le informazioni che cercano, per prendere rapidamente decisioni più smart basate su dati effettivi.

Conclusione

Non buttate soldi al vento dopo il verificarsi di un problema, e non aspettatevi che i team IT e Sicurezza possano fare miracoli senza le risorse e le capacità necessarie. Implementate una solida strategia di sicurezza informatica per concentrarvi sugli aspetti fondamentali per il business. Quindi, scegliete soluzioni create per rispondere alle esigenze di sicurezza fondamentali e proteggete il vostro ambiente dalle minacce informatiche sempre più evolute e diffuse.



www.ivanti.com



1.800.982.2130



sales@ivanti.com

1 Privacy Rights Clearinghouse

2 <https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/>

3 Verizon 2016 Data Breach Investigations Report (DBIR)

4 EY's Global Information Security Survey 2016-17

5 Studio di 2016 IBM X-Force, <http://www-03.ibm.com/press/us/en/pressrelease/51230.wss>

6 Op. cit.

7 Verizon 2017 DBIR

8 Verizon 2016 DBIR

9 <http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/>

10 <https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/>

11 <https://www.infosecurity-magazine.com/news/fedex-notpetya-cost-us-300-million/>

12 <http://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html>

13 http://files.shareholder.com/downloads/ABEA-3GG91Y/5005768664x0x954059/3E9E6E5C-7732-4401-8AFE-F37F7104E2F7/Maersk_Interim_Report_Q2_2017.pdf

14 <https://www.cisecurity.org/controls/>