Come mettere in ginocchio un'azienda (italiana) a colpi di click

Andrea Zwirner

andrea@linkspirit.it

@AndreaZwirner

Andrea Zwirner

- Mi interesso di sicurezza informatica dallo scorso millennio
  - “Connettere” significava “intrecciare”
  - Hacker non aveva ancora alcun significato

- Ho fondato Linkspirit, azienda che si occupa di
  - Consulenza nella progettazione sicura di software e sistemi
  - Verifiche di sicurezza su software e sistemi
  - Formazione in materia di sicurezza informatica

Cosa faccio

- Partecipo a diversi progetti liberi legati la divulgazione della cultura sulla sicurezza informatica

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

www.isecom.org

Hacker Highschool
SECURITY AWARENESS FOR TEENS

www.hackerhighschool.org


OWASP
The Open Web Application Security Project

www.owasp.org

Progetto scuole logo wanted! :-) www.progettoscuole.it

Di cosa parliamo oggi

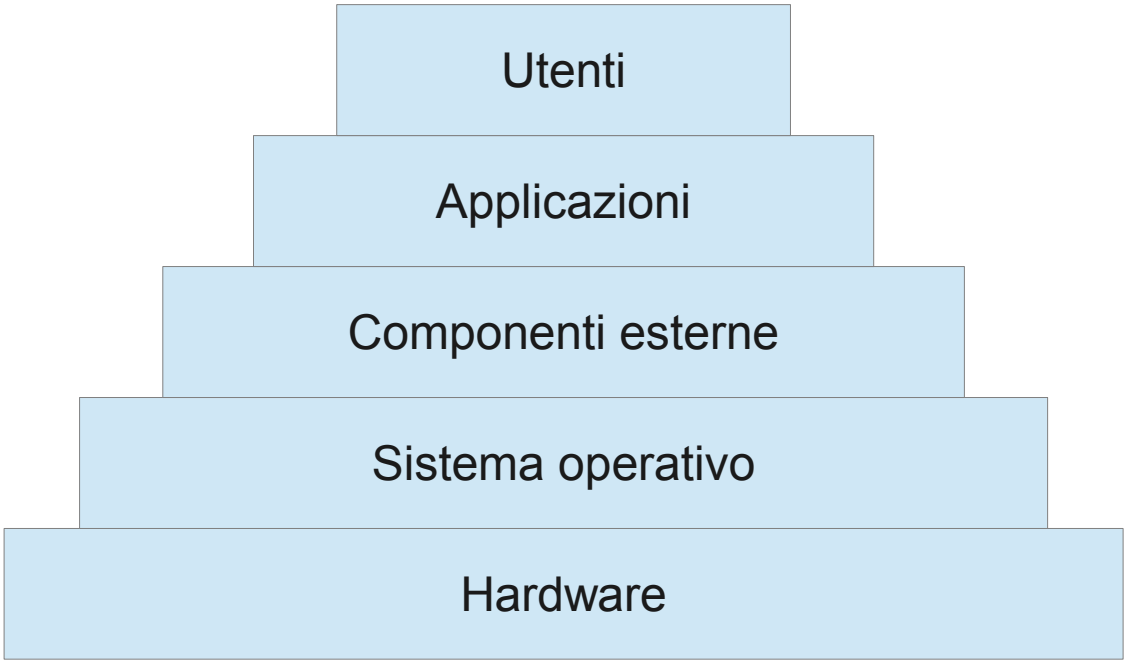
- Attacchi informatici a piccole e medie imprese
  - Motivazioni
  - Analisi dei vettori d'attacco
    - Componenti tecnologiche
    - Componenti sociali e culturali
  - Linee guida per la protezione

Motivazioni

- Furto di informazioni
- Furto di competenze
- Accesso a risorse di calcolo o di rete
- Accesso ai servizi aziendali
- Ricatti / Estorsioni

- Acquisizione di qualunque informazione possa avere un valore sul mercato nero
  - Dati di persone, documenti, dati bancari, carte di credito

Vettori d'attacco



Vettori d'attacco tecnologici

- L'attacco è condotto sfruttando vulnerabilità di software o sistemi
  - Applicazioni progettate o scritte in modo non sicuro
  - Utilizzo di componenti non sicure
  - Utilizzo errato di componenti sicure
  - Errata configurazione di applicativi, componenti esterne o sistemi operativi
  - Mancata messa in sicurezza di applicativi, componenti o sistemi

Software progettato in maniera non sicura

Privacy

[redacted]

Tel [redacted]
Fax [redacted]
Partita IVA [redacted]
E-Mail [redacted]
Sito Web [redacted]

Iscritto: Camera Commercio di Udine e Registro Imprese di [redacted] con nr. [redacted] in data [redacted]
Capitale sociale: [redacted] euro interamente versato

Informativa ex art. 13 D.lgs. 196/2003

Spett.le cliente, La informo che il D.lgs. n. 196 del 30 giugno 2003 (Codice in materia di protezione dei dati personali) prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. La scrivente Società informa che per l'instaurazione e l'esecuzione dei rapporti contrattuali/commerciali/informativi con Lei in corso entrerà/è in possesso di dati acquisiti anche verbalmente direttamente o tramite terzi, a Lei relativi, dati qualificati come personali dalla legge.
Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti. Ai sensi dell'articolo 13 del D.lgs. n.196/2003, pertanto, Le fornisco le seguenti informazioni:
I dati vengono raccolti e trattati per registrare il cliente ed attivare nei suoi confronti il servizio informativo richiesto nonchè per ogni altra eventuale e successiva esigenza contrattuale/commerciale nonchè per ottemperare ai conseguenti obblighi legali e contrattuali nonchè per conseguire una efficace gestione dei rapporti commerciali ed anche ai fini della tutela del credito e della migliore gestione dei nostri diritti relativi al singolo rapporto.
I dati da Lei forniti saranno utilizzati, per un periodo massimo di due anni dal Suo ultimo contatto, anche per l'invio periodico di documentazione/informazioni commerciali relative agli aggiornamenti delle tariffe e delle offerte praticate dall'intestata Società. In qualunque momento Lei comunque potrà opporsi al suddetto invio comunicandolo nei modi che riterrà a Lei più comodi.
I dati verranno trattati in forma scritta e/o su supporto magnetico, elettronico o telematico. Il conferimento dei dati stessi è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali/informativi e pertanto l'eventuale rifiuto a fornirli o al successivo trattamento potrà determinare l'impossibilità della scrivente a dar corso ai rapporti contrattuali/informativi medesimi.
Il mancato conferimento, invece, di tutti i dati che non siano riconducibili ad obblighi legali o contrattuali verrà valutato di volta in volta dalla scrivente e determinerà le conseguenti decisioni rapportate all'importanza dei dati richiesti rispetto alla gestione del rapporto commerciale.
Ferme restando le comunicazioni e diffusioni effettuate in esecuzione di obblighi di legge, i dati potranno essere eventualmente comunicati in Italia a:

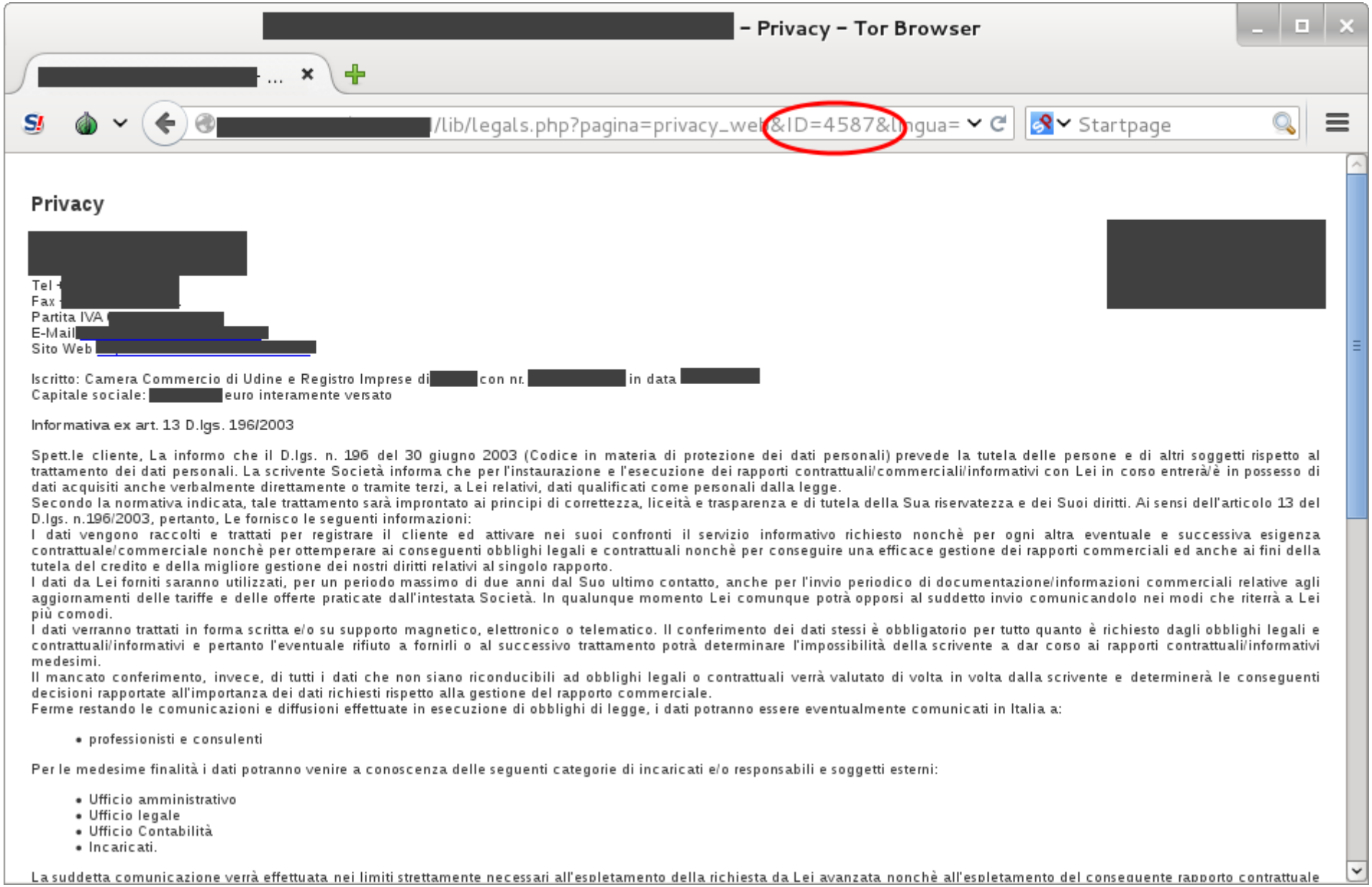
- professionisti e consulenti

Per le medesime finalità i dati potranno venire a conoscenza delle seguenti categorie di incaricati e/o responsabili e soggetti esterni:

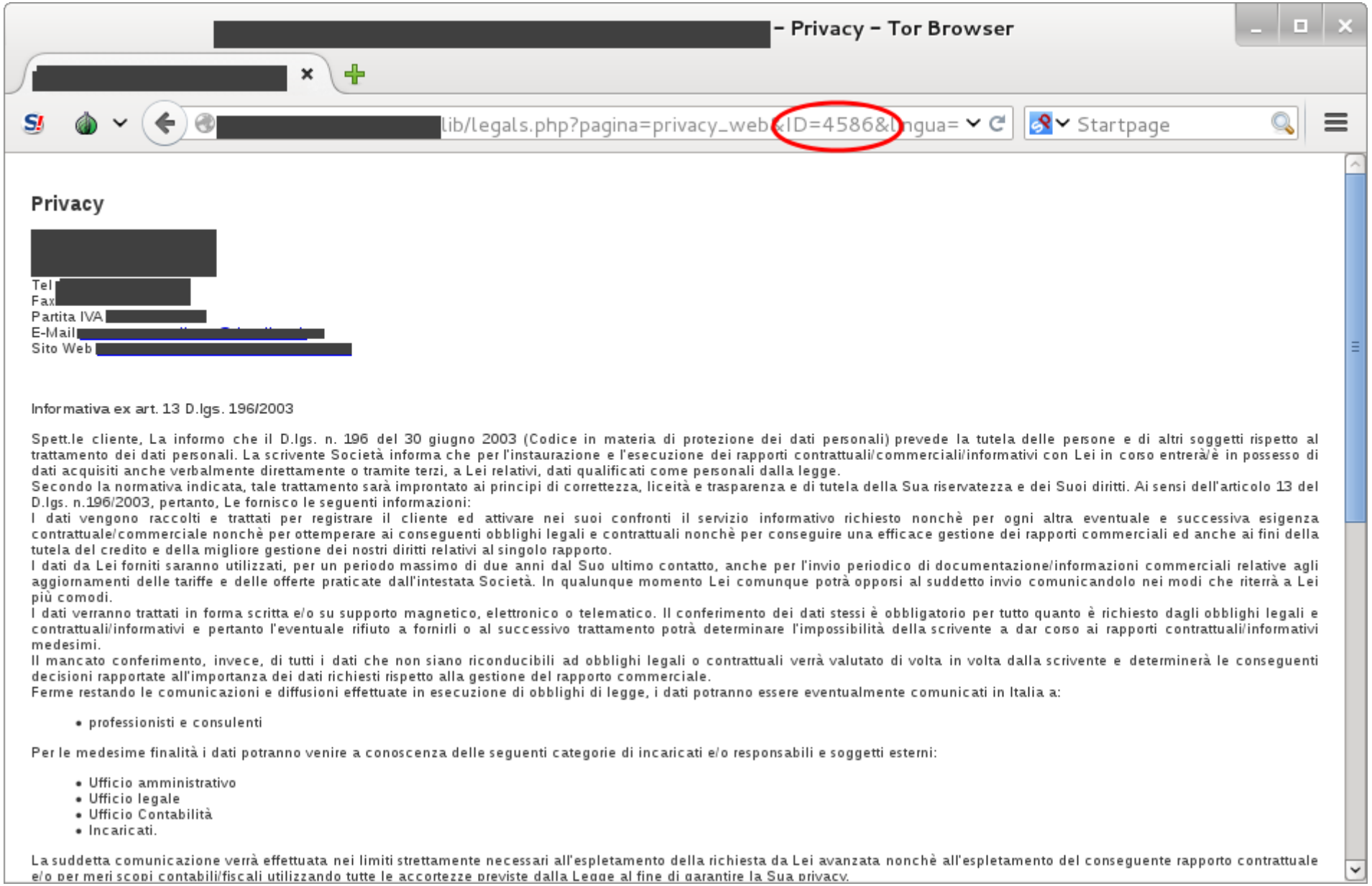
- Ufficio amministrativo
- Ufficio legale
- Ufficio Contabilità
- Incaricati.

La suddetta comunicazione verrà effettuata nei limiti strettamente necessari all'espletamento della richiesta da Lei avanzata nonchè all'espletamento del conseguente rapporto contrattuale

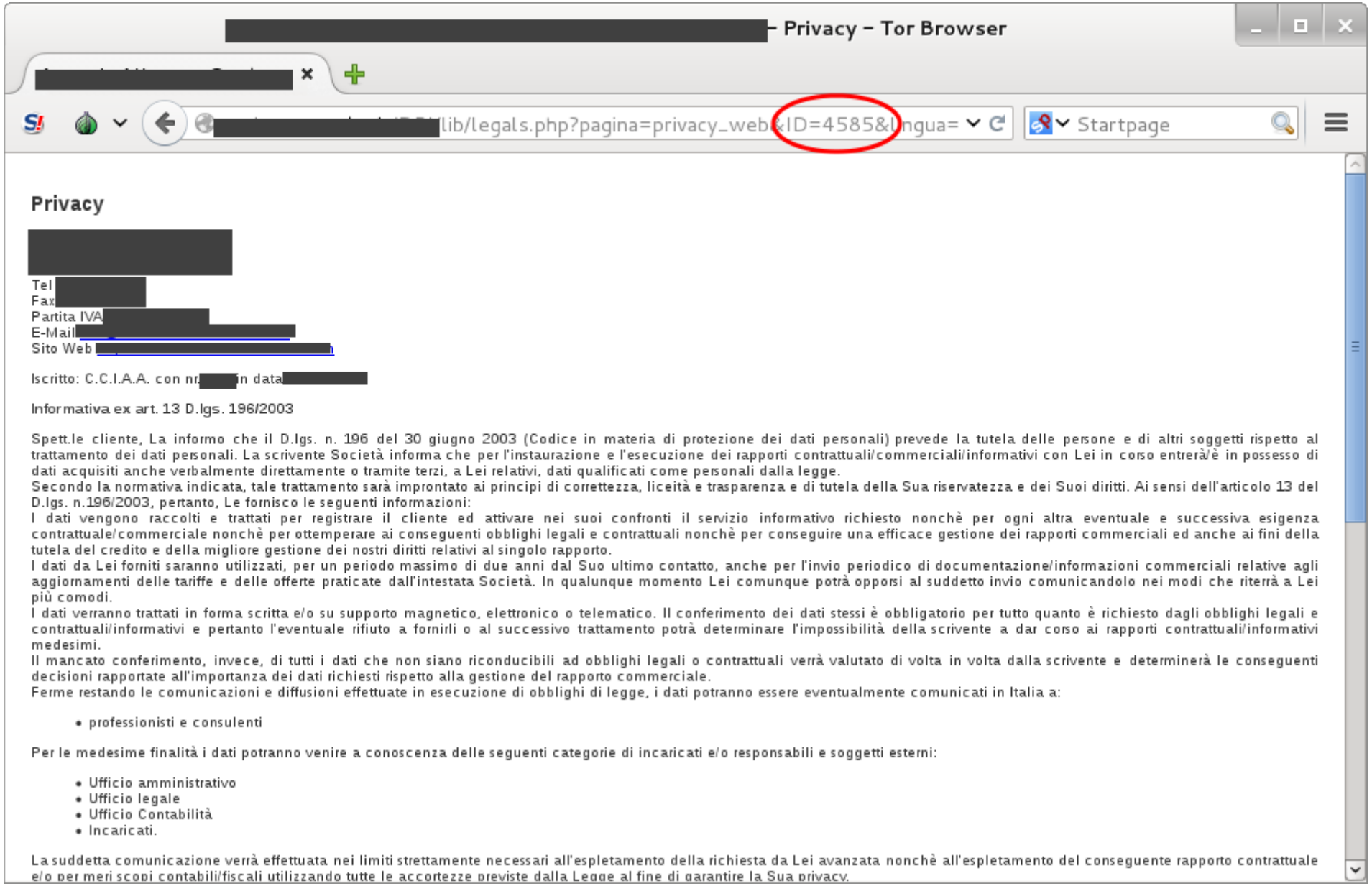
Software progettato in maniera non sicura



Software progettato in maniera non sicura



Software progettato in maniera non sicura



Privacy

[redacted]

Tel [redacted]
Fax [redacted]
Partita IVA [redacted]
E-Mail [redacted]
Sito Web [redacted]

Iscritto: C.C.I.A.A. con nr [redacted] in data [redacted]

Informativa ex art. 13 D.lgs. 196/2003

Spett.le cliente, La informo che il D.lgs. n. 196 del 30 giugno 2003 (Codice in materia di protezione dei dati personali) prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. La scrivente Società informa che per l'instaurazione e l'esecuzione dei rapporti contrattuali/commerciali/informativi con Lei in corso entrerà/è in possesso di dati acquisiti anche verbalmente direttamente o tramite terzi, a Lei relativi, dati qualificati come personali dalla legge.
Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti. Ai sensi dell'articolo 13 del D.lgs. n.196/2003, pertanto, Le fornisco le seguenti informazioni:
I dati vengono raccolti e trattati per registrare il cliente ed attivare nei suoi confronti il servizio informativo richiesto nonchè per ogni altra eventuale e successiva esigenza contrattuale/commerciale nonchè per ottemperare ai conseguenti obblighi legali e contrattuali nonchè per conseguire una efficace gestione dei rapporti commerciali ed anche ai fini della tutela del credito e della migliore gestione dei nostri diritti relativi al singolo rapporto.
I dati da Lei forniti saranno utilizzati, per un periodo massimo di due anni dal Suo ultimo contatto, anche per l'invio periodico di documentazione/informazioni commerciali relative agli aggiornamenti delle tariffe e delle offerte praticate dall'intestata Società. In qualunque momento Lei comunque potrà opporsi al suddetto invio comunicandolo nei modi che riterrà a Lei più comodi.
I dati verranno trattati in forma scritta e/o su supporto magnetico, elettronico o telematico. Il conferimento dei dati stessi è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali/informativi e pertanto l'eventuale rifiuto a fornirli o al successivo trattamento potrà determinare l'impossibilità della scrivente a dar corso ai rapporti contrattuali/informativi medesimi.
Il mancato conferimento, invece, di tutti i dati che non siano riconducibili ad obblighi legali o contrattuali verrà valutato di volta in volta dalla scrivente e determinerà le conseguenti decisioni rapportate all'importanza dei dati richiesti rispetto alla gestione del rapporto commerciale.
Ferme restando le comunicazioni e diffusioni effettuate in esecuzione di obblighi di legge, i dati potranno essere eventualmente comunicati in Italia a:

- professionisti e consulenti

Per le medesime finalità i dati potranno venire a conoscenza delle seguenti categorie di incaricati e/o responsabili e soggetti esterni:

- Ufficio amministrativo
- Ufficio legale
- Ufficio Contabilità
- Incaricati.

La suddetta comunicazione verrà effettuata nei limiti strettamente necessari all'espletamento della richiesta da Lei avanzata nonchè all'espletamento del conseguente rapporto contrattuale e/o per meri scopi contabili/fiscali utilizzando tutte le accortezze previste dalla Legge al fine di garantire la Sua privacy.

Quindi cosa si può fare?

- Enumerazione dei clienti dell'azienda che sono stati inseriti nella base dati per la generazione delle pagine Privacy

- L'uso che se ne può voler fare

Cos'è successo nel caso dell'

Assalto informatico all'Ass 4: c'è la denuncia alla Procura

L'Azienda sanitaria si è rivolta alla magistratura per far luce sulla diffusione dei reclami on line. Intanto il servizio è stato sospeso. E Insiel è al lavoro per mettere in sicurezza il sistema

internet sanità ass

di Cristian Rigo

UDINE. L'Azienda sanitaria numero 4 del Medio Friuli ha presentato una denuncia/querela alla Procura per far luce sull'assalto informatico che ha portato alla diffusione in rete di 129 reclami con tanto di nome, cognome e patologia dei pazienti e dei medici ritenuti responsabili di disservizi più o meno gravi. Una violazione della privacy senza precedenti nella sanità friulana per la quale però l'Ass 4, che nel frattempo ha sospeso il servizio, si considera parte lesa.

«Ci siamo rivolti alla magistratura - dice il direttore amministrativo Saverio Merzliak - perché ci riteniamo parte lesa. Qualcuno ha recuperato dal nostro sito informazioni riservate con dati sensibili e poi su un periodico web di informazione (dovatu.it, *ndr*) è stato pubblicato un link che consentiva a chiunque si collegasse di leggere questi dati. I casi sono due - aggiunge -: o siamo stati vittima di un attacco hacker, oppure il nostro sito non aveva protezioni adeguate. Saranno la Procura e le forze dell'ordine a valutare, ma in entrambi i casi la nostra azienda ha subito un danno. E lo stesso vale per i cittadini che hanno presentato un reclamo e per i medici che venivano chiamati in causa».

Dove stava la problematica?

http://portale.ass4.sanita.fvg.it /servlet /page ? _pageid=90 &
_dad=portal34 & _schema=PORTAL34 & act=17 & id=XXXX

Ma com'è possibile?

- Qualcuno è stupito che si trovino errori così banali in applicazioni che trattano dati tanto delicati?
- Sbagliare è umano, ma il problema è la tendenza delle aziende informatiche a lavorare alla “basta che funzioni”
- Devono chiudere e chiuderanno
- Ma nel frattempo non bisogna dar loro la possibilità di danneggiare le imprese. Ne terremo conto.

Dove hanno cercato di farci credere che

Gelocal Messaggero Veneto

+13°C
NUBI SPARSE
E SCHIARITE

Assalto informatico, Insiel: noi parte lesa

L'azienda: c'è stata un'intrusione nei nostri sistemi informatici. E la polizia postale ha sentito dovatu.it

pirati informatici | insiel | aziende sanitarie

+T -T

UDINE. Anche Insiel si considera parte lesa e annuncia possibili azioni legali. La società informatica ha infatti diffuso una nota in cui precisa che «in merito alla vicenda relativa alla diffusione in rete dei reclami presentati alla Azienda sanitaria 4 Medio Friuli attraverso la sezione del sito a ciò dedicata, si pone in rilievo che gli illeciti commessi consistono unicamente nell'accesso abusivo a sistemi informatici, nella diffusione consapevole dei dati raccolti e nella pubblicazione delle modalità di reperimento degli stessi».

In buona sostanza Insiel se la prende con chi si è accorto del sistema per poter leggere tutti i reclami (il presunto hacker) e poi ha diffuso le modalità di reperimento degli stessi e cioè il periodico on line dovatu.it. Proprio ieri il direttore di dovatu.it, Tommaso Botto è stato ascoltato dalla Polizia postale e ha poi precisato, sempre attraverso il sito che «dovatu.it non ha ricevuto querele né è indagato, ma è stato sentito come informato sui fatti (giustamente) e ha fornito tutti i particolari, anche non pubblicati sinora».

Ha poi aggiunto che «non c'è stato nessun hacker, nessun sabotaggio, nessuna craccatura, nessun assalto ai computer». In buona sostanza dovatu.it avrebbe ricevuto delle segnalazioni e poi denunciato «la precarietà del sistema».

Stefano Smania · ★ Top Commentator · Lavora presso Ospedale Santa Maria della Misericordia di Udine

Insiel parte lesa? ma se siete una manica di incompetenti, dovreste vergognarvi ed andarvene tutti a casa!!! Se sporgete querela verso quel povero ragazo che non ha fatto nulla di che, giuro che pubblico online centinaia di foto dei bachi dei vostri sistemi, e tutta la raccolta di referti malformati che girano per le nostre aziende....vergognatevi!!! Ve lo tiro io su un polverone che farebbe saltare molte teste. Vi pagano per un lavoro che non sapete fare, dovreste solo che chiedere scusa pubblicamente per la vostra ignoranza!!!!!

Rispondi · Mi piace · 8 · 11 ottobre 2013 alle ore 3.50

Angie Devetti Duratti

All'armi all'armi!!

Rispondi · Mi piace · 11 ottobre 2013 alle ore 4.43

Luigi Blarasin · Lavora presso Ass 6 friuli occidentale

Stefano se chiedessi i danni per tutte le ore di clinica che in pronto soccorso perdiamo per far girare il giocattolo informatico che vi hanno fornito chiuderebbe la regione, non la ditta di informatica

Rispondi · Mi piace · 2 · 11 ottobre 2013 alle ore 5.09

Massimiliano Don · Pediatra presso Ospedale Civile San Daniele del Friuli (UD)

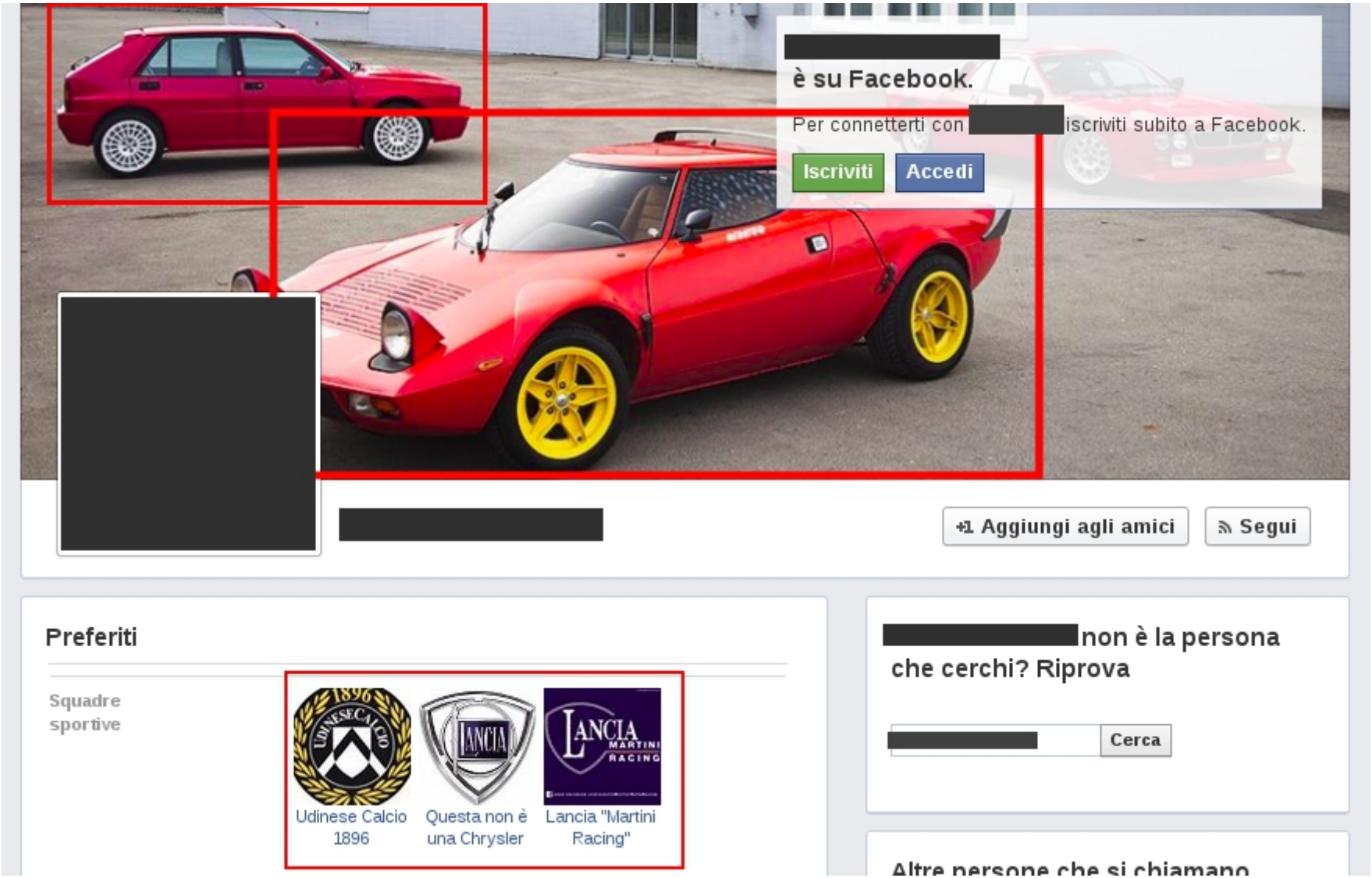
Fantastico Ste... io ti appoggio, di brutto !!!!!!

Rispondi · Mi piace · 11 ottobre 2013 alle ore 8.31

Vettori d'attacco culturali

- L'attacco è condotto sfruttando la componente umana
  - Curiosità
  - Interessi personali
  - Ignoranza
  - …
- Che diventano veicolo per l'esecuzione di software malevoli sulle postazioni di lavoro
- E' coadiuvato dal piacere diffuso del parlare di se o degli altri

Pagina facebook di Giovanni



Gruppi cui aderisce Giovanni

Giovanni e l'azienda X

- Giovanni è dipendente dell'azienda X

- L'obiettivo dell'attaccante sono dati riservati dell'azienda X (clienti e commesse, ad esempio)

Giovanni e l'azienda X

- Giovanni è dipendente dell'azienda X
- L'obiettivo dell'attaccante sono dati riservati dell'azienda X (clienti e commesse, ad esempio)
- Come pensate potrebbe agire?

Pianificazione dell'attacco: raccolta di informazioni

- Giovanni ama le auto, il rally e rimpiange i tempi del “turbo vecchia maniera”

- Supponiamolo interessato all'acquisto di un usato

Pianificazione dell'attacco: la trappola

- L'attaccante prepara un sito dove pubblica documenti relativi una falsa auto in vendita
- Le pagine web sfruttano le più recenti vulnerabilità dei software per la navigazione Internet
- I documenti informativi sfruttano le più recenti vulnerabilità dei software per la loro lettura
- L'attaccante convoglia Giovanni nella trappola via mail o con risposta diretta su form o social network

Assurdo?

- E' un attacco (da manuale) realmente avvenuto
- La passione erano i francobolli
- Il bersaglio ne cercava uno specifico per la sua collezione
- Lo ha scritto su un forum dedicato alla filatelia
- Ha ricevuto l'invito a cadere in trappola
- Ha fatto click.

Quindi cosa succede?

- Controllo della postazione di lavoro e suo utilizzo come:
  - ponte verso l'interno dell'azienda
    - Lettura del traffico nella rete interna (mail, raccolta password, ascolto VoIP, etc)
    - Attacco diretto delle altre postazioni in rete
    - Attacco diretto ai servizi informatici aziendali
  - base d'attacco verso altri obiettivi
    - Attacco diretto ai servizi di clienti e fornitori
- Un attacco mirato ha sempre un fine ben preciso

Vettori d'attacco culturali: casi più semplici

- L'attaccante “perde” un chiave USB infetta nel parcheggio dipendenti dell'azienda X. Cosa succederà?

Vettori d'attacco culturali: casi più semplici

- L'attaccante “perde” un chiave USB infetta nel parcheggio dipendenti dell'azienda X. Cosa succederà?

- L'attaccante invia direttamente a Giovanni una mail con allegato il software malevolo. Che cosa succederà?

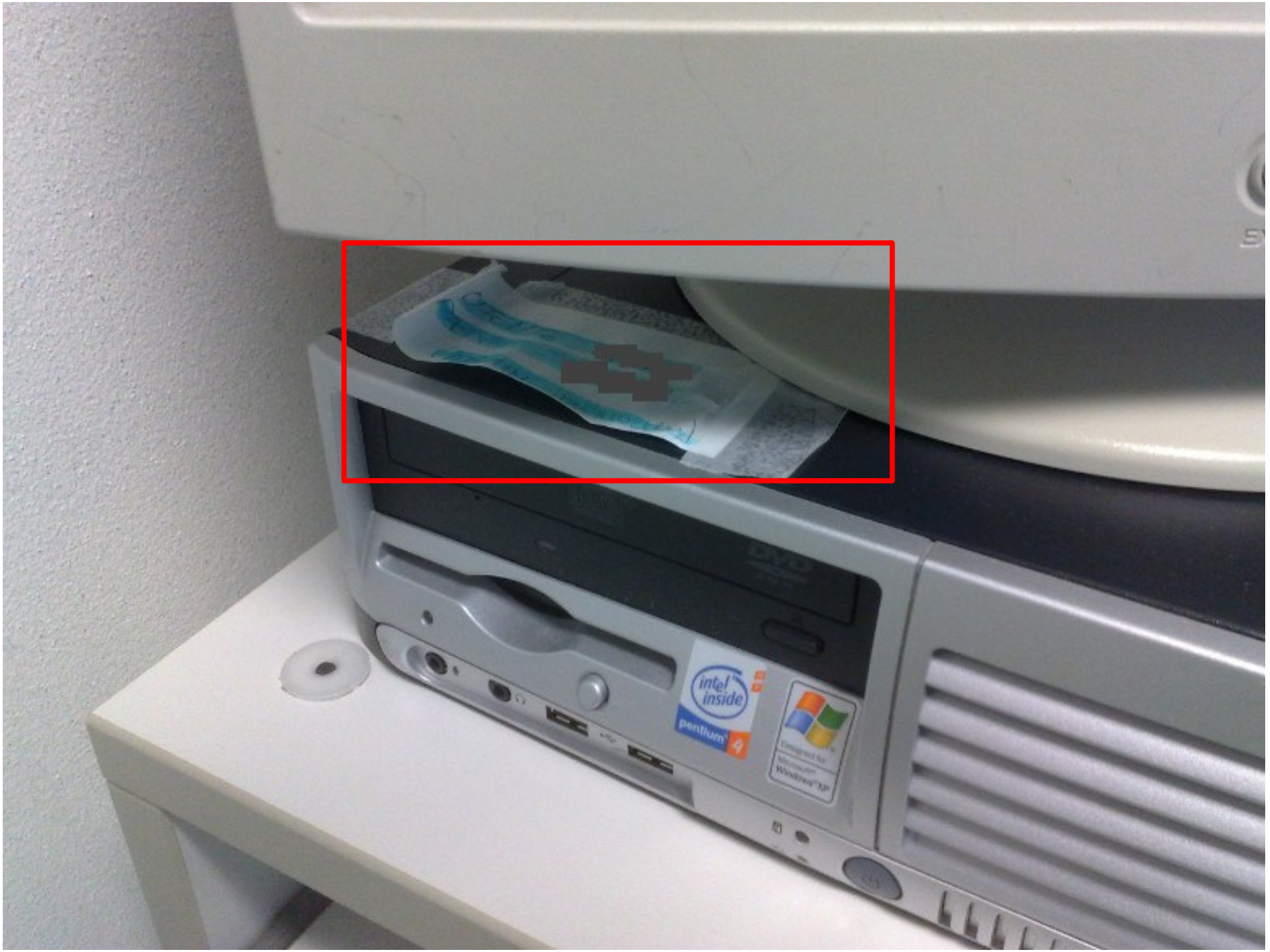
Vettori d'attacco culturali: casi più semplici

- L'attaccante “perde” un chiave USB infetta nel parcheggio dipendenti dell'azienda X. Cosa succederà?
- L'attaccante invia direttamente a Giovanni una mail con allegato il software malevolo. Che cosa succederà?
- Chi trova questi scenari un po' troppo surreali?


Surgifix
146
13


acer
Naturex 626
surgifix


intel inside
pentium 4


intel inside
pentium 4

TorrentLocker 2

Linee guida per proteggersi

- Possiamo immaginare la sicurezza informatica come una catena composta da anelli tecnologici ed anelli umani
- Portare a buon fine un attacco informatico significa riuscire a rompere questa catena
- Una catena è resistente quanto il suo anello più debole
- L'anello più debole della catena è la componente umana

Da cosa dobbiamo liberarci

Linee guida per proteggersi

Il problema non è tecnologico, ma culturale!

La strategia europea

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE OF THE
EUROPEAN UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

Consapevolezza

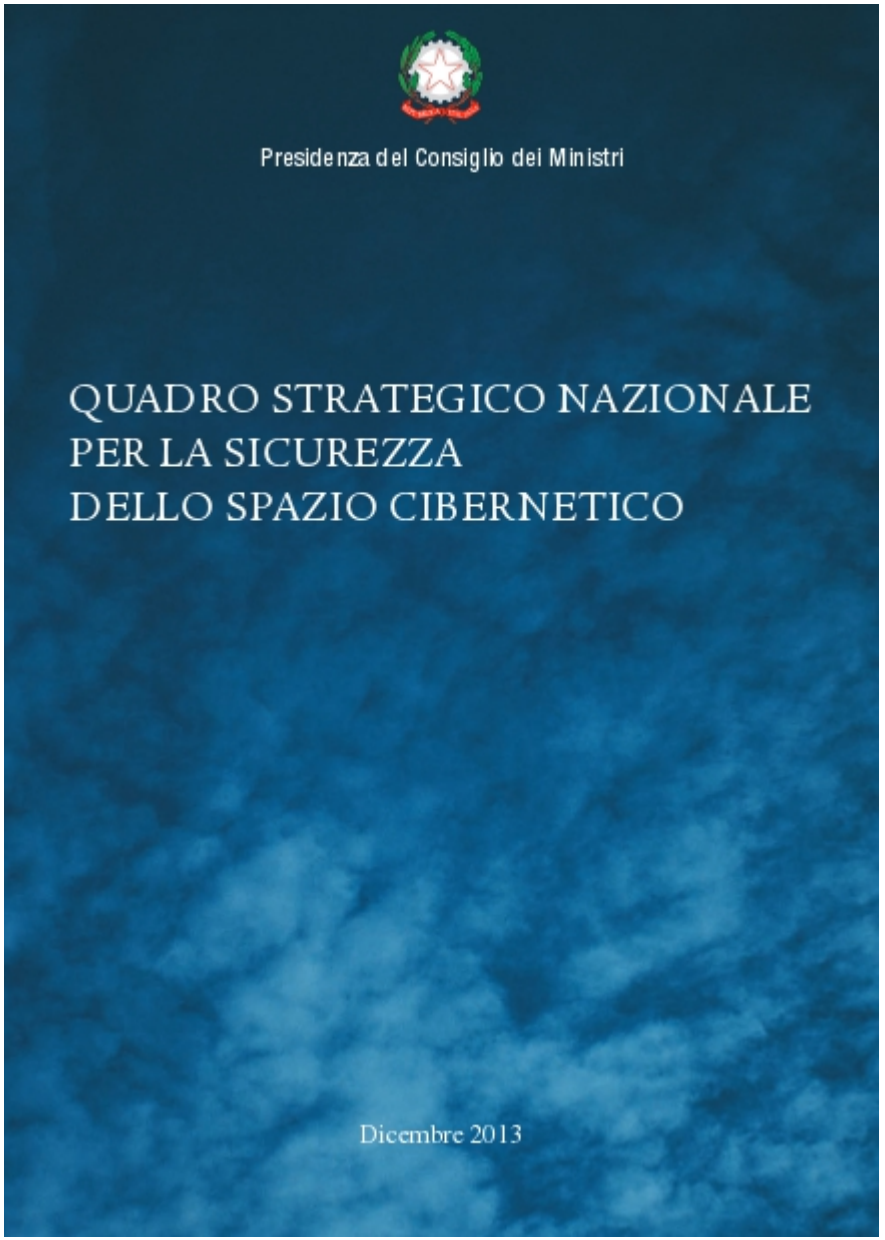
Se non si coinvolgono gli utenti, ogni sforzo è vano

"*Ensuring cybersecurity is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them.*"

Cybersecurity Strategy of the European Union

Commissione europea, febbraio 2013

La strategia italiana



Consapevolezza

"[…] *al fine di rafforzare le capacità nazionali di prevenzione, reazione e ripristino* […] *individua come nodi primari* […]:

p*romozione e diffusione della cultura della sicurezza cibernetica sia tra i cittadini che all'interno delle istituzioni [...] al fine di accrescere il livello di consapevolezza e di conoscenza della minaccia e dei relativi rischi*"

Quadro strategico nazionale per la sicurezza dello spazio cibernetico

Presidenza del Consiglio dei Ministri, dicembre 2013

Linee guida per proteggersi: aspetti culturali

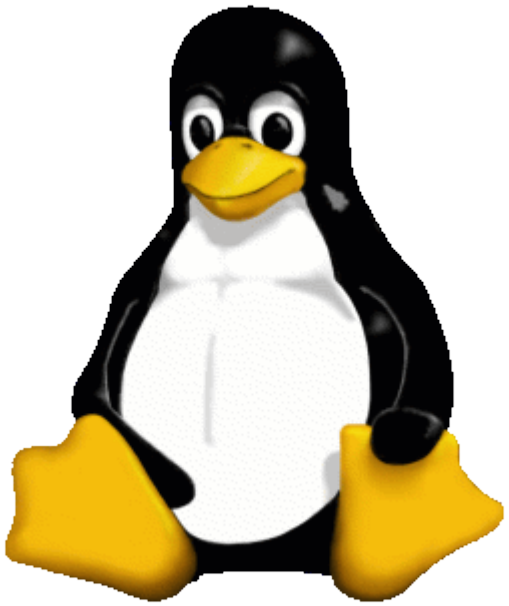
- Fare formazione ed aggiornamento per poter fare un uso consapevole degli strumenti informatici
- Non fare uso promiscuo personale/lavorativo degli strumenti informatici
- Cliccare responsabilmente: fare click su un collegamento sottende un legame di fiducia
- Scegliere password complesse e diverse per ogni servizio: quello con meno controlli può dare accesso agli altri

Linee guida per proteggersi: aspetti culturali

- Curare la propria “impronta digitale”
  - Evitare di pubblicare su Internet ogni particolare della propria esistenza: se so dove sei in ogni momento, so quando posso venire a svaligiarti casa!

- Non credere che un dispositivo o un software (e.g. firewall o antivrus) facciano La Sicurezza: la sicurezza è un processo

- Usare il buon senso, nella vita cosa c'è gratis?



Linee guida per proteggersi: aspetti tecnologici

- Definire tempi, procedure ed un responsabile per l'aggiornamento dei sistemi
- Regolamentare chiaramente l'utilizzo di Internet in azienda
- Selezionare ed installare solo applicazioni considerate affidabili e la cui installazione risulti indispensabile
- Configurare gli account degli utenti affinché abbiano i privilegi minimi richiesti per eseguire le attività loro assegnate

Linee guida per proteggersi: aspetti tecnologici

- Predisporre una difesa del perimetro della rete mediante strumenti informatici volti ad analizzare e proteggere in tempo reale il traffico di rete

- Impiegare sistemi automatizzati di analisi e filtro dei contenuti web, al fine di impedire la visualizzazione e la navigazione di siti Internet inappropriati e/o potenzialmente pericolosi

L'effetto valanga

- L'ignoranza generale sull'argomento, ha portato al dilagare di una piaga terribile fra le aziende che fanno informatica: la negligenza

- Nel mondo di servizi e prodotti informatici i concetti di contratto e di responsabilità sembrano non esistere.

  - Si usano ancora contratti degli anni '80 in cui il software è venduto “AS IS”, senza alcuna garanzia di funzionamento.
  - visto, piaciuto = se non funziona, affari tuoi. Se vuoi che lo sistemi c'è un (ingente) costo aggiuntivo. Sempre che sia d'accordo a sistemarlo.

Linee guida per proteggersi: aspetti tecnologici

- Richiedere specifiche garanzie di sicurezza ai fornitori di prodotti hardware e software
  - Esistono standard appositi da citare nei capitolati!
- Contrattualizzare con questi ultimi modalità e tempi di fornitura degli aggiornamenti di sicurezza
- L'interconnessione facilita il business come la propagazione di software malevoli: richiedere ai propri fornitori di applicare le medesime regole.

Come mettere in ginocchio un'azienda (italiana) a colpi di click

Andrea Zwirner

andrea@linkspirit.it

@AndreaZwirner