

# Informationssäkerhet

- två vanliga fenomen:  
identitetsstöld och bluffakturor

2015-09-16

-Lund-

Advokatfirman VICI

## Inledning och bakgrund

- Historisk dimension
  - Industrialismen
  - "IT-eran"
- Dokumentation
  - Manuella åtgärder
  - Digitala åtgärder
- Informationshantering
  - Fysisk lagring
  - Digital lagring
- Kommunikation och distribution
- IT-revolutionen

Advokatfirman VICI

## Identitetsstöld – vad är det?

- Identitet
  - Information för igenkänning av viss person
  - Juridisk och fysisk
- Information
  - Namn, firma, person- och organisationsnummer, adress, telefonnummer, e-postadress, ip-adress, dna, fingeravtryck, kontonummer (jfr personuppgifter)
  - Unik eller icke-unik; person- och organisationsnummer är unika, annan information i regel inte unik
- ”Stöld”
  - Som utgångspunkt ett fysiskt tillgrepp
  - Dagligt tal: bereder sig tillgång till ID-information

## Förfarande

- Identitetshandling
  - Körkort, ID-kort, pass
  - Genom stöld, borttappad/upphittad
- Betalkort
  - Kredit- och debetkort
- Både i fysisk och digital miljö
  - Fysisk miljö normalt sett svårare om erforderliga kontroller görs
  - Digital miljö förutsätter någon form av ”anonymitet”, vilket kan underlätta för brottslig verksamhet
- Dataintrång
  - Mobila enheter
  - Publika nätverk (exempel: försvarskonferensen)

## **Förfarande, forts.**

- Straffrättslig sida: bedrägeri, urkundsförfalskning, dataintrång m.m.
- Vardagskonsumtion
  - Förevisande av identitetshandling
  - Utnyttjande av bankkort
  - Falsk signatur
- Större inköp
  - Avvikande inköpsmönster kan upptäckas

## **Hur vet jag att min identitet har blivit kapad?**

- Kan vara svårt att upptäcka – konsekvenser kan inträffa lång tid efter gärningen
- Bank eller annat kreditinstitut tar kontakt
  - Avvikande inköpsmönster
  - Märklig geografisk lokalisering
- Information om kreditupplysningar
  - Ofta ett flertal under förhållandevis kort tid
  - Transaktioner redan genomförda
- Den stackars kollegan

## Åtgärder

- Kreditspär
  - Begärs hos kreditupplysningsföretag
  - Nackdel: kan inte ta egna krediter under den tid spärren finns
- Spärr av bankkort
- Kontakt med ”nya” kreditgivare – ev. bestrida fakturor
- Byta samtliga lösenord – telefon, dator, PIN-koder m.m. – ofta oklart hur gärningsmannen fått åtkomst till informationen
- Kontakta försäkringsbolag?
- Polisanmälan

Advokatfirman VICI

## Förebyggande åtgärder

- Företaget - internt
  - Verksamhetstyp – olika verksamheter kräver olika hänsyn
  - Särskilt skyddsvärd information – företagshemligheter
  - Anställd personal
  - Anlitad kompetens – konsulter m.fl.
  - Styrelse och ägare
- Företaget - externt
  - Kontakter med samarbetspartners, leverantörer, kunder, investerare, ägare m.fl.
  - Kommunikationskanaler – brev, telefax, telefon, e-post, gemensam/delad plattform
  - Segmentera information utifrån skyddsvärde/känslighet och välj kommunikationskanal därefter

Advokatfirman VICI

## **Förebyggande åtgärder, forts.**

- Hantering av koder och lösenord
- Försiktighet i digital miljö
  - Kontroll av hemsidor, leverantörer, betallösningar m.m.
  - PSI DSS – certifiering av säker digital betallösning
  - Distribution av känslig information – fysiskt eller digitalt
  - Publika nätverk och offentliga miljöer
- Försäkring
  - Försäkringsbolag börjar erbjuda ID-skydd som ett moment i försäkringen
  - Handlar till stor del om hjälp med hanteringen

Advokatfirman VICI

## **Bluffakturor**

- Vad är en s.k. bluffaktura?
  - Anmodan om betalning som saknar grund
  - Påstående om beställd vara eller tjänst
  - Distribueras ofta via post men även e-post
- Förövarstrategier
  - Nyttjande av kända varumärken
  - Massutskick – statistiskt säkerställd betalning
  - Hot om inkasso och Kronofogdemyndigheten med betalningsanmärkningar som följd
  - Insatser riktade mot enskilda – påstående om bevis för avtal
  - Småbelopp – brottsoffret upplever det som enklare att betala än att ta strid

Advokatfirman VICI

## **Bluffakturor, forts.**

- Hur bör en bluffaktura hanteras?
  - Bestridande av vilket det klart och tydligt framgår att man motsätter sig betalningsansvar och gärna med en kortfattad motivering
  - Bestridandet bör upprättas skriftligen och skickas med t.ex. e-post eller fax. Ett skriftligt bestridande utgör bevis för att bestridande de facto ägt rum.
  - Eventuellt polisanmälan
- Inkasso, Kronofogdemyndigheten, betalningsanmärkningar m.m.
  - Ett förfarande vid Kronofogdemyndigheten förutsätter att den aktuella fordran är *klar* och *förfallen*
  - En stridig (bestriden) fordran kan aldrig ligga till grund för ett betalningsföreläggande/utslag från Kronofogdemyndigheten

Advokatfirman VICI

## **Bluffakturor, forts.**

- Inkasso, Kronofogdemyndigheten, betalningsanmärkningar m.m., forts.
  - Betalningsanmärkning kan därför inte heller komma ifråga (dock juridiska personer)
  - Bluffaktureringsföretag påstår ofta motsatsen
  - Hänvisade till allmän domstol
  - Lågre belopp – inte full ersättning för rättegångskostnad

Advokatfirman VICI



### **Lite om s.k. skimning (kortkapning)**

- Vanligtvis smygekopiering av bankkort
- Otillåten avläsningsenhet i anslutning till legitim kortterminal
- Kopiering av magnetremsa och/eller chip – chip dock betydligt svårare
- Avläsning av inpräglad information (bl.a. cvv-kod) – Internetköp
- Förfrågan om information via e-post (bank, Skatteverket, Polismyndigheten etc.)

Advokatfirman VICI



### **Lite om s.k. skimning (kortkapning), forts.**

- Kortinnehavaren ansvarar endast för egna uttag/betalningar
- Borttappat kort – grov vårdslöshet
- Äkta kort försett med vattenstämpel – möjligt att i efterhand avgöra om uttag/köp är obehörigt
- Mer riskfyllda miljöer: vissa platser utomlands, Internet
- Kreditkort istället för debetkort
- Kontroll av webbsidor, ständig uppsyn

Advokatfirman VICI

## Något om informationssäkerhet i företag

- Företagets interna förhållanden
  - Verksamheten
  - Företagshemligheter
  - Ägare, styrelse, personal
- Företagets externa förhållanden
  - Samarbetspartners, leverantörer, kunder, investerare, ägare m.fl.
  - Kommunikationskanaler – brev, telefax, telefon, e-post, gemensam/delad plattform

Advokatfirman VICI

## Skyddsstruktur

- Allmän - lagstiftning
  - Främst lagen (1990:409) om företagshemligheter ("FHL")
  - Med "företagshemlighet" avses (1 § FHL): *sådan information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för honom i konkurrenshänseende*
  - **Affärs- eller driftförhållande:** kan vara all information med anknytning till ett företag; affärshändelser, marknadsundersökningar, prissättningskalkyler, planerade aktiviteter, marknadsplanering, pågående drift och produktion, konstruktionsarbete, utveckling, forskning, prover, administrativa förhållanden
  - **Håller hemlig:** inte tillgänglig för envar som vill ta del av den, ambition att hålla informationen inom den krets för vilken den är känd
  - **Skada i konkurrenshänseende:** konkurrensförmågan ska påverkas i negativ riktning, utgångspunkt är en sund och effektiv konkurrens

Advokatfirman VICI



## Skyddsstruktur, forts.

- Enskild
  - Avtal
    - Skriftliga avtal med IT-konsulter, anställd personal, anlitad kompetens, styrelseledamöter m.fl.
    - Sekretess
    - Vite
  - IT-miljö
    - Infrastruktur med väl anpassad säkerhetsnivå
    - Servrar, arbetsstationer, telefoner, surfplattor, skrivare, nätverk (gäst och arbete)
    - Antivirusprogramvara, brandväggar, proxy
    - Behörighetsnivåer
  - IT-policy
    - Bindande för alla
    - Reglera användning av information
    - Reglera användning av infrastruktur

## Skyddsstruktur, forts.

- Enskild, forts.
  - IT-revision
    - Säkerhetsexpert för teknisk kontroll av anlitad IT-konsult
    - Genomgång av juridisk struktur i IT-miljön



## **VICI:s IT-revision**

- Ändamål och syfte
  - Ge en samlad bild av och struktur i den befintliga IT-miljön
- Resultat
  - Påvisa säkerhetsbrister
  - Konkreta förslag på åtgärder
  - Rekommendationer
- En juridisk/legal del
- En teknisk del (samarbete med IXX IT-partner AB)

Advokatfirman VICI



## **VICI:s IT-revision, forts.**

- Den legala delen
  - Genomgång och analys av befintliga avtal och policies
  - Fokus på avtal med IT-konsulter, anställd personal och andra konsulter
  - Interna processer, informationssegmentering
- Den tekniska delen
  - Genomförs av en anlitad säkerhetsexpert (IT-säkerhet)
  - Säkerhetskontroll av IT-miljö och infrastruktur
  - Säkerhetsbrister (tekniska) ådagaläggs
- Slutrapport
  - Beskrivning av befintlig IT-miljö och infrastruktur
  - Redogörelse för den juridiska undersökningen och analysen
  - Redogörelse för den tekniska säkerhetskontrollen
  - Redovisning av resultat
  - Slutsatser, rekommendationer och åtgärdsförslag

Advokatfirman VICI

## **Sammanfattning**

- Identitetsstöld och bluffakturor blir allt vanligare
- Förebyggande åtgärder i kombination med skyndsamt agerande
  - Policies i företaget, skapa medvetenhet, identifiera just dina riskmiljöer, försäkring, säker IT-infrastruktur
  - Dokumenterad åtgärdsplan – bestridande av fakturor, polisanmälan, kontakt med försäkringsbolag – ”tid är pengar”
- Skimming
  - Särskilda riskmiljöer
  - Kreditkort kontra debetkort (bestridande av faktura)

## **Sammanfattning, forts.**

- IT-säkerhet på företaget
  - Ordentliga avtal och policies
  - Dokumentera en informationsrutin eller -policy
  - Implementera den med hänsyn tagen till innehållet i FHL och befintliga avtal
  - IT-infrastruktur
- Nyttan av en ordentlig IT-revision
  - Klar och tydlig bild
  - Underlag för framtida beslut



## **Kontaktuppgifter**

Christian Karlsson  
[ck@vici.se](mailto:ck@vici.se)  
073-204 23 40

Advokatfirman VICI