COMPUTER CRIMES – REATI INFORMATICI

I Computer Crimes sono i reati che hanno 2 elementi o implicano l'uso di uno strumento informatico oppure coinvolgono un apparato informatico come oggetto che viene su cui ricade l'azione commessa dal soggetto agente : o è la pistola con cui si spara (lo strumento) o è l'oggetto che subisce l'evento criminoso.
I Computer Crimes sono disciplinati dal codice penale.
Art. 615 ter. DA IMPARARE A MEMORIA.
Parola chiave: "abusivamente".
L'art. Si compone di 2 tipologie di eventi differenti (in gergo tecnico: fattispecie)
- *Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza* …….se il sistema non ha protezioni di sicurezza l'accesso non configura reato.
- *ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*…...Quando un dipendente accede regolarmente ed il titolare per esempio lo licenzia, il dipendente non può più accedere ai sistemi aziendali.

Per il reato sono previsti dei casi che configurano delle aggravanti:

- se lo stesso reato è compiuto da una persona con determinate caratteristiche (elementi soggettivi)
- o l'evento si è consumato in una determinata situazione (elementi oggettivi)

la pena può essere aumentata (non si configurano 2 reati, ma l'aggravamento della pena dell'unico reato).
SLIDE 5 – Policy aziendale rilevante per definire "l'abuso della qualità di operatore del sistema" (il regolamento definisce cosa l'operatore di sistema può/deve o non può/non deve fare).
SLIDE 6 – punto 2) è difficile da configurare in ambiente informatico.

SLIDE 7 - punto 3.

Per alcuni reati solo il soggetto che subisce il danno può far partire l'iter del procedimento, così per i computers crime.
Il pubblico ufficiale non può far partire alcun procedimento se non c'è querela.
Nel caso in cui si configurino le aggravanti il pubblico ufficiale può procedere d'ufficioanche se non c'è querela (15:50 – risentilo perché non ho capito bene).
"… Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio."

CASI CONCRETI – SENTENZE

CASO 1 – danneggiava i dati sostituendo il file.

CASO 2 – tecnicamente il dipendente poteva accedere (non siamo nel primo caso), ma nella seconda parte della frase della SLIDE 4 si dice: **si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.**

DANNEGGIAMENTO INFORMATICO
Art. 635 bis del codice penale.
(non citare il numero degli articoli se non si è sicuri della correttezza- importanti sono le definizione ed il contenuto degli articoli, il significato).

Bis e ter sono dei latinismi usati dal legislatore che, molto tempo dopo dalla promulgazione della legge, effettua delle precisazioni o delle specificazioni (in questo caso è intervenuta un'evoluzione tecnologica).
Nel momento in cui si configura una nuova fattispecie di reato deve essere aggiunto alla previsione di legge per evitarne l'estensione per analogia che la materia penale non ammette.

"in tutto o in parte" è valido anche sotto il profilo temporale:

- in tutto = sempre
- in parte = temporaneamente

CASO 3 – Il lavoratore è ancora dipendente quando cancella i dati.
Il dipendente impugna il licenziamento perché puntava sul fatto che i dati non erano andati persi, ma erano stati recuperati.
Se si da il connotato giuridico "chiunque rende in tutto o in parte" (per un po' di tempo) si ha la condanna e comunque il reato informatico è un reato di pura condotta (non è necessario l'evento).

CASO 4 – Chi invia la mail contenente il virus senza saperlo e volerlo non è colpevole (non c'è alcun tipo di illecito) proprio per effetto dell'automatismo degli accadimenti della fattispecie.
L'invio è automatico, non c'è intervento cosciente della persona fisica.