Da: IT-Grundschutz Kompendium Edition 2023
Traduzione di Marco Tomazzoni - Traduzione non ufficiale, solo a scopo informativo.

Contenuto

G 0.1 Fuoco....3
G 0.2 Condizioni climatiche avverse....4
G 0.3 Acqua....5
G 0.4 Inquinamento, polvere, corrosione....6
G 0.5 Catastrofi naturali....7
G 0.6 Disastri nei dintorni....8
G 0.7 Eventi di rilievo nei dintorni....9
G 0.8 Interruzione o malfunzionamento dell'alimentazione....10
G 0.9 Interruzione o malfunzionamento delle reti di comunicazione....12
G 0.10 Interruzione o malfunzionamento delle reti di fornitura....13
G 0.11 Interruzione o malfunzionamento dei fornitori di servizi....15
G 0.12 Disturbi elettromagnetici....17
G 0.13 Intercettazione di radiazioni compromettenti....18
G 0.14 Spionaggio....19
G 0.15 Intecettazioni....20
G 0.16 Furto di apparecchiature, supporti dati o documenti....21
G 0.17 Perdita di apparecchiature, supporti dati o documenti....22
G 0.18 Pianificazione errata o mancanza di adattamento....23
G 0.19 Divulgazione di informazioni meritevoli di protezione....25
G 0.20 Informazioni o prodotti da fonti inaffidabili....27
G 0.21 Manipolazione di hardware e software....28
G 0.22 Manipolazione di informazioni....29
G 0.23 Intrusione non autorizzata nei sistemi informatici....30
G 0.24 Distruzione di apparecchiature o supporti dati....31
G 0.25 Guasto di apparecchiature o sistemi....32
G 0.26 Malfunzionamento di apparecchiature o sistemi....33
G 0.27 Mancanza di risorse....34
G 0.28 Errori o punti deboli di software....35
G 0.29 Violazione di leggi o regolamenti....36
G 0.30 Utilizzo o amministrazione non autorizzata di apparecchiature e sistemi....38
G 0.31 Uso o amministrazione errata di apparecchiature e sistemi....39
G 0.32 Uso improprio delle autorizzazioni....40
G 0.33 Mancanza di personale....41
G 0.34 Attacchi....42
G 0.35 Coercizione, estorsione o corruzione....43
G 0.36 Furto d'identità....44
G 0.37 Diniego di azioni....45
G 0.38 Uso improprio di dati personali....46
G 0.39 Malware....47
G 0.40 Denial of Service....48

G 0.41 Sabotaggio....49
G 0.42 Social engineering....50
G 0.43 Manipolazione di messaggi....52
G 0.44 Ingresso non autorizzato....53
G 0.45 Perdita di dati....54
G 0.46 Perdita di integrità di informazioni riservate....55
G 0.47 Effetti collaterali dannosi di attacchi informatici....56

G 0.1 Fuoco

Gli incendi possono causare gravi danni alle persone, agli edifici e ai loro arredi. Oltre ai danni diretti causati dal fuoco, si possono individuare anche danni conseguenti, che possono raggiungere proporzioni catastrofiche, soprattutto per le tecnologie informatiche. I danni da acqua di spegnimento, ad esempio, non si verificano solo sul luogo dell'incendio. Possono verificarsi anche nelle zone più profonde dell'edificio. Quando il PVC brucia, si producono gas di cloro che, insieme all'umidità dell'aria e all'acqua di spegnimento, formano acido cloridrico. Se i vapori di acido cloridrico si disperdono attraverso il sistema di condizionamento dell'aria, possono causare danni alle apparecchiature elettroniche sensibili situate in una parte dell'edificio lontana dal luogo dell'incendio. Ma anche il "normale" fumo d'incendio può avere un effetto dannoso sulle apparecchiature informatiche.

Un incendio non è causato solo da una gestione negligente del fuoco (ad esempio, fiamme libere non sorvegliate, lavori di saldatura), ma anche dall'uso improprio di apparecchiature elettriche (ad esempio, macchina del caffè incustodita, sovraccarico di prese multiple). Anche i difetti tecnici degli apparecchi elettrici possono provocare un incendio.

La propagazione di un incendio può essere favorita, tra l'altro, da:

- trattenere le porte dei compartimenti antincendio con cunei,
- stoccaggio improprio di materiali combustibili (ad esempio carta straccia),
- mancata osservanza delle norme e dei regolamenti in materia di prevenzione degli incendi,
- mancanza di apparecchiature di rilevazione degli incendi (ad esempio, rilevatori di fumo),
- mancanza o inutilizzo di estintori portatili o di dispositivi di spegnimento automatico (ad esempio, impianti di estinzione a gas),
- protezione antincendio preventiva inadeguata (ad esempio, mancanza di barriere antincendio sui percorsi dei cavi o utilizzo di materiali isolanti non idonei per l'isolamento termico e acustico).

Esempi:

- All'inizio degli anni '90, un grande centro di calcolo nell'area di Francoforte ha subito danni catastrofici da incendio che hanno portato a un guasto completo.
- Capita spesso che piccoli apparecchi elettrici, come macchine da caffè o lampade da tavolo, vengano installati o predisposti in modo improprio, causando incendi.

G 0.2 Condizioni climatiche avverse

Condizioni climatiche sfavorevoli come il caldo, il gelo o l'elevata umidità possono causare danni di vario tipo, ad esempio malfunzionamenti dei componenti tecnici o danni ai supporti di memorizzazione. Le frequenti fluttuazioni delle condizioni climatiche intensificano questo effetto. Le condizioni ambientali sfavorevoli possono anche causare l'impossibilità di lavorare o addirittura infortuni o morti.

Ogni persona ed ogni dispositivo tecnico ha un intervallo di temperatura entro il quale può funzionare normalmente o il suo corretto funzionamento è garantito. Se la temperatura ambiente supera i limiti di questo intervallo verso l'alto o verso il basso, possono verificarsi interruzioni del lavoro, malfunzionamenti o guasti alle apparecchiature.

Le finestre delle sale server vengono spesso aperte senza autorizzazione per motivi di ventilazione. Nel periodo di transizione (primavera, autunno), le forti oscillazioni di temperatura possono portare al superamento dell'umidità dell'aria consentita a causa del forte raffreddamento.

Esempi:

- In piena estate e con un raffreddamento insufficiente, le apparecchiature IT possono subire guasti dovuti alla temperatura.
- La presenza di troppa polvere nei sistemi IT può causare un accumulo di calore.
- Le temperature eccessive possono smagnetizzare i supporti magnetici dei dati.

G 0.3 Acqua

L'acqua può compromettere l'integrità e la disponibilità delle informazioni memorizzate su supporti di dati analogici e digitali. Anche le informazioni contenute nella memoria di lavoro dei sistemi informatici sono a rischio. L'ingresso incontrollato di acqua negli edifici o nei locali può essere causato, ad esempio, da:

- difetti nell'approvvigionamento idrico o nello smaltimento delle acque reflue,
- difetti nell'impianto di riscaldamento,
- difetti negli impianti di condizionamento dell'aria con collegamento all'acqua,
- difetti negli impianti sprinkler,
- acqua di spegnimento durante le operazioni antincendio e
- sabotaggio dell'acqua, ad esempio aprendo i rubinetti e bloccando gli scarichi.

Indipendentemente dal modo in cui l'acqua penetra negli edifici o nei locali, esiste il rischio che le strutture di alimentazione o i componenti IT vengano danneggiati o messi fuori uso (cortocircuito, danni meccanici, ruggine, ecc.). Soprattutto se le strutture centrali di alimentazione dell'edificio (distributori principali per elettricità, telefono, dati) si trovano in locali seminterrati senza drenaggio automatico, l'acqua che penetra può causare danni molto elevati.

I problemi possono derivare anche dal gelo. Ad esempio, le tubature in zone soggette a gelo possono perdere se l'acqua si ferma durante il gelo prolungato. Anche l'isolamento termico esistente viene superato dal gelo con il passare del tempo.

Esempio:

- In una sala server, un tubo dell'acqua passava sotto il soffitto, coperto da elementi in cartongesso. Quando un raccordo del tubo dell'acqua ha iniziato a perdere, non è stato rilevato in tempo. L'acqua fuoriuscita si è raccolta dapprima nel punto più basso del rivestimento, per poi fuoriuscire e causare un cortocircuito nel distributore di corrente installato in basso. Di conseguenza, è stato necessario interrompere completamente l'erogazione dell'acqua e dell'elettricità nella parte interessata dell'edificio fino alla riparazione definitiva.

G 0.4 Inquinamento, polvere, corrosione

Oltre all'elettronica, molti dispositivi IT contengono anche componenti che funzionano meccanicamente, come dischi rigidi e rimovibili, unità DVD, stampanti, scanner e così via, ma anche ventole di processori e alimentatori. Con sempre maggiori esigenze di qualità e velocità, questi dispositivi devono funzionare con una precisione sempre maggiore. Anche la più piccola contaminazione può causare il malfunzionamento di un dispositivo. Polvere e contaminazione possono derivare, ad esempio, dalle seguenti attività:

- Lavori su pareti, pavimenti rialzati o altre parti dell'edificio,
- lavori di adeguamento dell'hardware,
- operazioni di disimballaggio delle unità (ad esempio, allontanamento del polistirolo).

I circuiti di sicurezza esistenti nelle unità di solito portano a un arresto tempestivo. In questo modo i danni diretti all'unità, i costi di riparazione e i tempi di inattività rimangono contenuti, ma l'unità interessata non è disponibile.

Anche le apparecchiature e le infrastrutture possono essere attaccate dalla corrosione. Questo può avere un impatto negativo non solo sull'IT, ma anche sulla sicurezza dell'edificio. La corrosione può anche causare indirettamente altri pericoli. Ad esempio, l'acqua può fuoriuscire dalle aree corrose (vedere G 0.3 Acqua).

In generale, la sporcizia, la polvere o la corrosione possono causare guasti o danni ai componenti IT e alle strutture di alimentazione. Di conseguenza, la corretta elaborazione delle informazioni può essere compromessa.

Esempi:

- Quando un server è stato installato in una sala multimediale, insieme a una fotocopiatrice e a un fax, si è verificata la paralisi della ventola del processore e della ventola dell'alimentatore, una dopo l'altra, a causa dell'elevato carico di polvere presente nella sala. Il guasto della ventola del processore ha causato sporadici crash del server. Il guasto della ventola dell'alimentatore ha infine portato al surriscaldamento dell'alimentatore con conseguente cortocircuito, che alla fine ha causato un guasto totale del server.
- Per appendere una lavagna a muro in un ufficio, il servizio tecnico ha praticato dei fori nella parete. I dipendenti avevano lasciato il proprio ufficio per un breve periodo di tempo. Una volta tornati sul posto di lavoro, uno dei PC non funzionava più. La causa era la polvere di perforazione che era entrata nell'alimentatore del PC attraverso le fessure di ventilazione.

G 0.5 Catastrofi naturali

Le catastrofi naturali sono cambiamenti naturali che hanno effetti devastanti sulle persone e sulle infrastrutture. Le cause di un disastro naturale possono essere fenomeni sismici, climatici o vulcanici, come terremoti, inondazioni, frane, tsunami, valanghe ed eruzioni vulcaniche. Esempi di fenomeni meteorologici estremi sono tempeste, uragani o cicloni. A seconda dell'ubicazione dell'organizzazione, la sua esposizione ai rischi derivanti dai vari tipi di disastri naturali varia notevolmente.

Esempi:

- Per i data center situati in aree a rischio di inondazione, esiste spesso un rischio particolare di penetrazione incontrollata dell'acqua nell'edificio (inondazione o innalzamento del livello delle acque sotterranee).
- La frequenza dei terremoti e quindi il rischio associato dipendono fortemente dalla posizione geografica.

Indipendentemente dal tipo di catastrofe naturale, anche nelle aree non direttamente colpite c'è il rischio che le strutture di approvvigionamento, le comunicazioni o i componenti IT vengano danneggiati o messi fuori uso. In particolare, il guasto alle strutture centrali di alimentazione degli edifici (distributori principali di elettricità, telefono e dati) può provocare danni molto elevati. Al personale operativo e di assistenza può essere negato l'accesso all'infrastruttura a causa della creazione di grandi aree interdette all'accesso.

Esempi:

- Molte imprese commerciali, anche di grandi dimensioni, non tengono sufficientemente conto del rischio di inondazioni. Ad esempio, un'azienda è già stata "sorpresa" diverse volte dai danni causati da un'alluvione al suo centro dati. Il centro dati è stato letteralmente spazzato via per la seconda volta nel giro di 14 mesi. I danni risultanti ammontano a diverse centinaia di migliaia di euro e non sono coperti da alcuna assicurazione.
- Un sistema informatico è collocato in un sito la cui posizione geografica è nota per l'attività vulcanica (fenomeno intermittente in cui si alternano fasi di emissione a periodi talvolta lunghi di quiescenza).

G 0.6 Disastri nei dintorni

Un ente pubblico o un'azienda possono subire danni se nelle vicinanze si verifica un grave incidente, ad esempio un incendio, un'esplosione, il rilascio di sostanze tossiche o la fuoriuscita di radiazioni pericolose. Il pericolo non deriva solo dall'evento in sé, ma anche dalle attività che spesso ne conseguono, come ad esempio le chiusure di aree o le misure di salvataggio.

Le proprietà di un'istituzione possono essere esposte a vari pericoli provenienti dall'ambiente circostante, tra cui il traffico (stradale, ferroviario, aereo, idrico), le aziende vicine o le aree residenziali.

Le misure di prevenzione o di salvataggio possono avere un impatto diretto sulle proprietà. Tali misure possono anche comportare l'impossibilità di raggiungere il posto di lavoro o l'evacuazione del personale. Tuttavia, la complessità dei servizi dell'edificio e delle strutture informatiche può comportare anche problemi indiretti.

Esempio:

- Un incendio in un impianto chimico nelle immediate vicinanze di un centro di calcolo (circa 1000 m. in linea d'aria) ha prodotto una potente nube di fumo. Il centro informatico era dotato di un sistema di condizionamento e ventilazione che non disponeva di un sistema di monitoraggio dell'aria esterna. Solo grazie all'attenzione di un dipendente (l'incidente è avvenuto durante l'orario di lavoro), che ha seguito la formazione e la diffusione, è stato possibile spegnere manualmente l'alimentazione di aria esterna in tempo.

G 0.7 Eventi di rilievo nei dintorni

I grandi eventi di ogni tipo possono ostacolare il corretto funzionamento di un'autorità o di un'azienda. Si tratta di feste di piazza, concerti, eventi sportivi, azioni sindacali o dimostrazioni. I disordini legati a tali eventi possono provocare ulteriori effetti, come l'intimidazione dei dipendenti fino all'uso della violenza contro il personale o l'edificio.

Esempi:

- Durante i caldi mesi estivi, si è svolta una manifestazione nei pressi di un centro dati. La situazione è degenerata e si sono verificati episodi di violenza. In una strada laterale, una finestra dell'area del centro dati era ancora aperta, attraverso la quale un dimostrante è entrato e ha colto l'occasione per rubare hardware con dati importanti.
- Durante la preparazione di una grande fiera, una linea elettrica è stata accidentalmente tagliata. Ciò ha provocato un guasto in un centro di calcolo alimentato da questa, che tuttavia è stato possibile limitare grazie al sistema di alimentazione di riserva disponibile.

G 0.8 Interruzione o malfunzionamento dell'alimentazione

Nonostante l'elevato livello di sicurezza dell'approvvigionamento, si verificano ripetutamente interruzioni della fornitura di energia elettrica da parte dei gestori delle reti di distribuzione (DSO) o delle aziende fornitrici di energia (utility). La maggior parte di queste interruzioni sono così brevi (meno di un secondo) che le persone non le notano. Tuttavia, anche le interruzioni di durata superiore a 10 ms sono in grado di interrompere le operazioni IT. Oltre ai disturbi nella rete di alimentazione, tuttavia, anche le interruzioni durante i lavori non annunciati o i danni ai cavi durante i lavori di ingegneria civile possono causare un'interruzione dell'alimentazione.

Non sono solo le ovvie utenze dirette (PC, illuminazione, ecc.) a dipendere dall'alimentazione elettrica. Oggi molte infrastrutture dipendono dall'elettricità, ad esempio gli ascensori, la tecnologia di climatizzazione, i sistemi di allarme, i cancelli di sicurezza, i sistemi di chiusura automatica delle porte e gli impianti sprinkler. Anche l'approvvigionamento idrico nei grattacieli dipende dall'elettricità a causa delle pompe necessarie per generare pressione ai piani superiori. In caso di interruzioni di corrente prolungate, il guasto delle infrastrutture può comportare l'impossibilità di svolgere attività nei locali interessati.

Oltre alle interruzioni, anche altri guasti all'alimentazione possono influire sulle operazioni. La sovratensione, ad esempio, può causare malfunzionamenti o addirittura danni alle apparecchiature elettriche.

Va inoltre notato che le interruzioni di corrente o i disturbi nelle vicinanze possono avere ripercussioni anche sui processi aziendali, ad esempio se le vie di accesso sono bloccate.

Esempi:

- A causa di un guasto nell'UPS di un centro dati, non è stato possibile ripristinare il normale funzionamento dopo una breve interruzione di corrente. Dopo aver scaricato le batterie (dopo circa 40 minuti), tutti i computer della sala server interessata si sono guastati.
- All'inizio del 2001, in California si è verificata un'emergenza energetica durata oltre 40 giorni. La situazione dell'alimentazione era così tesa che l'Autorità di monitoraggio della rete californiana ordinò tagli di corrente a rotazione. Queste interruzioni di corrente, che duravano fino a 90 minuti, interessavano non solo le famiglie ma anche l'industria high-tech. Poiché con il blackout si sono spenti anche i

sistemi di allarme e le telecamere di sorveglianza, le aziende fornitrici di energia hanno tenuto segreti i loro piani di spegnimento.

- Nel novembre 2005, in seguito a forti nevicate in Bassa Sassonia e Nord Reno-Westfalia, molte comunità rimasero senza corrente per giorni perché molti tralicci dell'alta tensione erano caduti sotto il peso della neve e del ghiaccio. Ci sono voluti diversi giorni per ripristinare l'alimentazione elettrica.

G 0.9 Interruzione o malfunzionamento delle reti di comunicazione

Molti processi aziendali oggi richiedono collegamenti di comunicazione intatti almeno per una parte del tempo, sia tramite telefono, fax, e-mail o altri servizi su reti locali o ad ampio raggio. Se alcuni o diversi di questi collegamenti di comunicazione si guastano per un periodo di tempo prolungato, questo può portare, ad esempio, al fatto che:

- i processi aziendali non possono più essere elaborati perché non è possibile recuperare le informazioni necessarie,
- i clienti non riescono più a contattare l'istituto per le loro richieste,
- gli ordini non possono essere inviati o completati.

Se le applicazioni time-critical sono gestite da sistemi IT collegati tramite reti ad ampio raggio, il danno potenziale e i danni conseguenti causati da un guasto della rete sono elevati se non esistono opzioni di ripiego (ad esempio, la connessione a una seconda rete di comunicazione).

Problemi analoghi possono verificarsi se le reti di comunicazione necessarie sono disturbate ma non si guastano completamente. I collegamenti di comunicazione possono, ad esempio, presentare un tasso di errore maggiore o altre carenze qualitative. Anche i parametri di funzionamento errati possono causare problemi.

Esempi:

- Internet è diventato oggi un mezzo di comunicazione indispensabile per molte organizzazioni, tra l'altro per il reperimento di informazioni importanti, per la presentazione all'esterno e per la comunicazione con la clientela e altri soggetti. Le aziende specializzate in servizi basati su Internet dipendono ovviamente in modo particolare da una connessione Internet funzionante.
- Per la convergenza delle reti, i servizi voce e dati vengono spesso trasportati attraverso gli stessi componenti tecnici (ad esempio, il VoIP). Tuttavia, questo aumenta il rischio che i servizi vocali e i servizi dati si guastino contemporaneamente in caso di interruzione della tecnologia di comunicazione.

G 0.10 Interruzione o malfunzionamento delle reti di fornitura

In un edificio esiste un gran numero di reti che servono per i basilari approvvigionamenti e smaltimenti e quindi servono da base per tutti i processi aziendali di una organizzazione, compresa l'informatica. Esempi di tali reti di alimentazione sono:

- Elettricità,
- telefono,
- raffreddamento,
- riscaldamento e/o ventilazione,
- acqua e fognature,
- approvvigionamento idrico per l'antincendio,
- gas,
- sistemi di segnalazione e controllo (ad esempio per sistemi antifurto, antincendio, di gestione degli edifici) e
- sistemi di interfono.

Il guasto o l'interruzione di una rete di fornitura può, tra l'altro, comportare l'impossibilità per le persone di lavorare nell'edificio o la compromissione delle operazioni informatiche e quindi dell'elaborazione delle informazioni.

Le reti dipendono in varia misura l'una dall'altra, per cui le interruzioni operative di ogni singola rete possono ripercuotersi anche sulle altre.

Esempi:

- Un guasto al riscaldamento o alla ventilazione può costringere tutti i dipendenti a lasciare gli edifici interessati. In determinate circostanze, ciò può comportare danni elevati.
- L'interruzione dell'alimentazione elettrica non ha un effetto diretto solo sull'IT, ma anche su tutte le altre reti dotate di tecnologia di controllo e regolazione a comando elettrico. Anche le condutture fognarie possono contenere pompe di sollevamento elettriche.

- L'interruzione dell'approvvigionamento idrico può influire sul funzionamento dei sistemi di condizionamento dell'aria.

G 0.11 Interruzione o malfunzionamento dei fornitori di servizi

Quasi nessuna organizzazione oggi lavora senza fornitori in outsourcing, società di servizi o di fornitura. Quando le unità organizzative dipendono da fornitori di servizi, il fallimento dei servizi esterni può influire sull'esecuzione dei compiti. Il fallimento parziale o totale di fornitori di servizi di outsourcing o di aziende fornitrici può avere un impatto significativo sulla continuità operativa, soprattutto per i processi aziendali critici. Le cause di tali fallimenti possono essere diverse, come l'insolvenza, la risoluzione unilaterale del contratto da parte del fornitore di servizi o delle aziende fornitrici, problemi operativi dovuti, ad esempio, a forze naturali o ad assenze del personale. I problemi possono sorgere anche se i servizi forniti dalle società di servizi non soddisfano i requisiti di qualità del cliente.

Va inoltre notato che i fornitori di servizi ricorrono spesso a subappaltatori per fornire i loro servizi al cliente. Le interruzioni, le carenze qualitative e i fallimenti dei subappaltatori possono quindi portare indirettamente a danni per il cliente.

Anche i processi aziendali delle amministrazioni aggiudicatrici possono essere compromessi da guasti dei sistemi informatici dei fornitori di servizi o dei collegamenti di comunicazione con essi.

Il necessario recupero dei processi esternalizzati può essere molto difficile, ad esempio perché i processi esternalizzati non sono sufficientemente documentati o perché i precedenti fornitori di servizi non supportano il recupero.

Esempi:

- Un'azienda ha installato i propri server in un centro dati di una società di servizi esterna. In seguito a un incendio in questo centro dati, il reparto finanziario dell'azienda non è stato più in grado di agire. L'azienda ha subito notevoli perdite finanziarie.
- La produzione just-in-time di un'azienda dipendeva dalla fornitura di risorse operative da parte di società di servizi esterne. Dopo la rottura di un camion a causa di un difetto della società di servizi, la consegna dei pezzi urgentemente necessari ha subito un drastico ritardo. Di conseguenza, gran parte della clientela non ha potuto essere rifornita in tempo.
- Un istituto bancario gestiva tutti i trasporti di contante con una società di cash-in-transit. L'azienda di trasporto contanti ha inaspettatamente presentato istanza di fallimento. Ci sono voluti diversi giorni per prendere accordi e pianificare i percorsi

con una nuova società di cash-in-transit. Di conseguenza, si sono verificati notevoli problemi e ritardi nella e ritardi nella fornitura e nello smaltimento del contante alle filiali bancarie.

G 0.12 Disturbi elettromagnetici

Oggi la tecnologia dell'informazione è costituita in gran parte da componenti elettronici. Sebbene la tecnologia di trasmissione ottica sia sempre più utilizzata, i computer, gli elementi di accoppiamento di rete e i sistemi di archiviazione, ad esempio, contengono solitamente molti componenti elettronici. Le radiazioni di interferenza elettromagnetica che agiscono su tali componenti possono compromettere il funzionamento dei dispositivi elettronici o addirittura danneggiarli. Di conseguenza, possono verificarsi guasti, malfunzionamenti, risultati di elaborazione errati o errori di comunicazione. o si possono verificare errori di comunicazione.

Anche la comunicazione wireless può essere influenzata dalle interferenze elettromagnetiche. In determinate circostanze, un'interferenza sufficientemente forte delle bande di frequenza utilizzate è sufficiente per questo.

Inoltre, le informazioni memorizzate su alcuni tipi di supporti dati possono essere cancellate o falsificate dalle interferenze elettromagnetiche. Questo vale in particolare per i supporti dati magnetizzabili (dischi rigidi, nastri magnetici, ecc.) e le memorie a semiconduttore. È anche possibile danneggiare tali supporti dati con le radiazioni di interferenza elettromagnetica.

Esistono diverse fonti di campi elettromagnetici o radiazioni, ad esempio reti radio come WLAN, Bluetooth, GSM, UMTS, eccetera, i magneti permanenti e le radiazioni cosmiche. Inoltre, ogni dispositivo elettrico emette onde elettromagnetiche di maggiore o minore intensità, che possono propagarsi nell'aria e lungo i conduttori metallici (ad esempio, cavi, condotti dell'aria condizionata, tubi del riscaldamento, ecc.

In Germania, la Legge sulla Compatibilità Elettromagnetica delle Apparecchiature (EMVG) contiene norme in materia.

G 0.13 Intercettazione di radiazioni compromettenti

I dispositivi elettrici emettono onde elettromagnetiche. Nei dispositivi che elaborano informazioni (ad esempio, computer, monitor, elementi di interfaccia di rete, stampanti), queste radiazioni possono anche trasportare le informazioni elaborate. Queste radiazioni che trasportano informazioni sono chiamate radiazioni che espongono o compromettono. Gli aggressori che si trovano nella casa di un vicino o in un veicolo parcheggiato nelle vicinanze, ad esempio, possono cercare di ricevere questa radiazione e ricostruire le informazioni elaborate. La riservatezza delle informazioni è quindi messa in discussione. Un possibile obiettivo di questo tipo di attacco è lo spionaggio industriale.

I valori limite previsti dalla legge sulla compatibilità elettromagnetica delle apparecchiature (EMVG) non sono generalmente sufficienti a prevenire l'intercettazione di radiazioni esposte. Se questo rischio non può essere accettato, è quindi necessario adottare misure di protezione aggiuntive.

La esposizione di radiazioni non si limita alle onde elettromagnetiche. Informazioni utili possono essere ottenute anche dalle onde sonore, ad esempio dalle stampanti o dalle tastiere.

Va inoltre notato che in alcuni casi l'esposizione può essere causata o amplificata anche dalla manipolazione esterna delle apparecchiature. Ad esempio, se un dispositivo viene irradiato con onde elettromagnetiche, le onde riflesse possono contenere informazioni riservate.

G 0.14 Spionaggio

Lo spionaggio si riferisce agli attacchi che mirano a raccogliere, valutare ed elaborare informazioni su aziende, persone, prodotti o altri oggetti target. Le informazioni elaborate possono poi essere utilizzate, ad esempio, per dare a un'altra azienda determinati vantaggi competitivi, per ricattare le persone o per copiare un prodotto.

Oltre a una serie di attacchi tecnicamente complessi, spesso esistono metodi molto più semplici per ottenere informazioni preziose, ad esempio combinando informazioni provenienti da diverse fonti pubblicamente accessibili che singolarmente sembrano innocue ma che in altri contesti possono essere compromettenti. Poiché i dati riservati spesso non sono sufficientemente protetti, possono essere spiati con mezzi visivi, acustici o elettronici.

Esempi:

- Molti sistemi IT sono protetti contro l'uso non autorizzato da meccanismi di identificazione e autenticazione, ad esempio sotto forma di controlli del nome dell'account e della password. Tuttavia, se la password viene inviata in chiaro sulla linea, potrebbe essere possibile leggerla.
- Per prelevare denaro da un bancomat, è necessario inserire il PIN corretto per la carta di credito/debito utilizzata. Purtroppo, la protezione visiva di queste macchine è spesso insufficiente, per cui gli aggressori possono facilmente guardare alle spalle del cliente durante l'inserimento del PIN. Se poi gli aggressori rubano la carta, possono usarla per saccheggiare il conto.
- Per ottenere i diritti di accesso a un PC o per manipolarlo in altro modo, gli aggressori possono inviare all'utente un cavallo di Troia allegato a un'e-mail come programma apparentemente utile. Oltre al danno diretto, i cavalli di Troia possono essere utilizzati per spiare un'ampia varietà di informazioni non solo sul singolo computer, ma anche sulla rete locale. In particolare, molti cavalli di Troia mirano a spiare le password o altri dati di accesso.
- In molti uffici, le postazioni di lavoro non sono ben schermate acusticamente l'una dall'altra. Di conseguenza, altri dipendenti e visitatori possono ascoltare le conversazioni e venire a conoscenza di informazioni non destinate a loro o addirittura riservate.

G 0.15 Intecettazioni

L'intercettazione si riferisce ad attacchi mirati a collegamenti di comunicazione, conversazioni, fonti di rumore di ogni tipo o sistemi informatici per raccogliere informazioni. Si parte dall'intercettazione clandestina e inosservata di una conversazione fino ad arrivare ad attacchi altamente tecnici e complessi per intercettare segnali inviati via radio o linee, ad esempio con l'aiuto di antenne o sensori.

Non solo per il basso rischio di rilevamento, l'intercettazione di linee o connessioni radio è una minaccia alla sicurezza delle informazioni che non deve essere trascurata. Fondamentalmente, non esistono cavi a prova di intercettazione. L'unica differenza tra i cavi è lo sforzo necessario per intercettarli. Solo con un grande sforzo metrologico è possibile determinare se una linea è effettivamente sottoposta a intercettazione.

La trasmissione non protetta di dati di autenticazione è particolarmente critica con i protocolli di testo in chiaro come HTTP, FTP o Telnet, che sono facili da analizzare automaticamente grazie alla chiara strutturazione dei dati.

La decisione di intercettare le informazioni da qualche parte è determinata essenzialmente dalla domanda se le informazioni valgono lo sforzo tecnico o finanziario e il rischio di essere scoperte. La risposta a questa domanda dipende molto dalle possibilità e dagli interessi individuali degli attaccanti.

Esempi:

- Nel caso delle telefonate, non è solo l'intercettazione delle conversazioni che può interessare gli aggressori. Anche le informazioni trasmesse durante la segnalazione possono essere utilizzate impropriamente da terzi, ad esempio se la password viene trasmessa in chiaro durante il login a causa di un'impostazione errata del dispositivo terminale.
- In caso di trasmissione radio non protetta o non sufficientemente protetta (ad esempio, se una WLAN è protetta solo con WEP), l'intera comunicazione può essere facilmente intercettata.
- Le e-mail possono essere lette durante tutto il loro percorso attraverso la rete se non sono criptate. Le e-mail non crittografate non dovrebbero quindi essere paragonate alle classiche lettere, ma alle cartoline.

G 0.16 Furto di apparecchiature, supporti dati o documenti

Il furto di supporti dati, sistemi IT, accessori, software o dati comporta, da un lato, costi per la sostituzione e per il ripristino delle condizioni di funzionamento e, dall'altro, perdite dovute alla mancanza di disponibilità. Se a seguito del furto vengono divulgate informazioni riservate, ciò può comportare ulteriori danni. Oltre ai server e ad altri sistemi IT costosi, anche i sistemi IT mobili, poco appariscenti e facili da trasportare, vengono spesso rubati. Tuttavia, ci sono anche casi di furti mirati, in cui i supporti di dati, come i documenti o le chiavette USB, sono rubati appositamente per ottenere l'accesso alle informazioni riservate in essi contenute.

Esempi:

- Nella primavera del 2000, un notebook è scomparso dal Dipartimento di Stato americano. In una dichiarazione ufficiale, non è stato escluso che il dispositivo potesse contenere informazioni riservate. Non si sapeva nemmeno se il dispositivo fosse protetto dalla crittografia o da altre misure contro l'accesso non autorizzato.
- Un ufficio federale tedesco è stato violato più volte attraverso le stesse finestre non protette. Oltre ad altri oggetti di valore, sono scomparsi anche sistemi informatici mobili. Non si può escludere con certezza che i file siano stati copiati o manipolati.
- Nel Regno Unito, si sono verificate diverse violazioni di dati in cui sono stati esposti documenti confidenziali a causa del furto di supporti dati. In un caso, sono stati rubati diversi dischi rigidi di computer dall'aeronautica militare britannica, che contenevano informazioni molto personali raccolte per l'autorizzazione di sicurezza dei dipendenti.
- Diversi dipendenti di un call center hanno fatto copie di una grande quantità di dati riservati dei clienti poco prima di dover lasciare l'azienda. Dopo aver lasciato l'azienda, i dipendenti hanno venduto questi dati ad aziende concorrenti. Poiché i dettagli dell'incidente sono stati successivamente divulgati alla stampa, il call center ha perso molti clienti importanti.

G 0.17 Perdita di apparecchiature, supporti dati o documenti

Ci sono molte cause che possono portare alla perdita di dispositivi, supporti dati e documenti. Questo influisce direttamente sulla disponibilità, ma le informazioni riservate possono anche cadere nelle mani di terzi, se i supporti dati non sono completamente crittografati. La sostituzione dei dispositivi o dei supporti dati comporta dei costi, ma anche quando ricompaiono, le informazioni potrebbero essere state divulgate o potrebbero essere stati installati programmi indesiderati.

Soprattutto i dispositivi mobili e i supporti dati mobili possono essere facilmente persi. Oggi, enormi quantità di dati possono essere memorizzate su piccole schede di memoria. Tuttavia, capita anche che i documenti cartacei vengano accidentalmente dimenticati, ad esempio nei ristoranti o nei mezzi di trasporto.

Esempi:

- I dipendenti utilizzano il tram per raggiungere il posto di lavoro per consultare alcuni documenti. Quando scendono freneticamente alla fermata di destinazione, lasciano accidentalmente i documenti sul sedile vicino. Sebbene i documenti non siano confidenziali, è necessario ottenere nuovamente le firme di alcuni dirigenti di alto livello.
- In occasione di un evento importante, un dipendente lascia cadere accidentalmente e inosservato una scheda di memoria con calcoli riservati sul pavimento, mentre cerca nella sua valigetta. La persona che ha trovato la scheda di memoria visualizza il contenuto sul suo computer portatile e vende le informazioni alla concorrenza.
- Un'azienda invia per posta dei CD con aggiornamenti software per la risoluzione dei problemi alla sua clientela. Alcuni di questi CD vengono persi durante il trasporto, senza che l'azienda o i suoi clienti ne siano informati. Di conseguenza, i clienti interessati subiscono malfunzionamenti del software.

G 0.18 Pianificazione errata o mancanza di adattamento

Se i processi organizzativi che servono direttamente o indirettamente all'elaborazione delle informazioni non sono progettati correttamente, possono verificarsi problemi di sicurezza. Anche se ogni singola fase del processo viene eseguita correttamente, spesso si verificano danni perché i processi nel loro complesso non sono definiti correttamente.

Un'altra possibile causa di problemi di sicurezza sono le dipendenze con altri processi che di per sé non hanno una relazione evidente con le informazioni. Tali dipendenze possono essere facilmente trascurate in fase di pianificazione e quindi innescare problemi durante il funzionamento.

I problemi di sicurezza possono sorgere anche quando i compiti, i ruoli o le responsabilità non sono assegnati in modo chiaro. Ciò può causare, tra l'altro, un ritardo nei processi, la trascuratezza delle misure di sicurezza o l'inosservanza delle norme.

Il pericolo sussiste anche se le apparecchiature, i prodotti, le procedure o altri mezzi per realizzare l'elaborazione delle informazioni non vengono utilizzati in modo appropriato. La scelta di un prodotto inadatto o le carenze nell'architettura dell'applicazione o nella progettazione della rete, ad esempio, possono causare problemi di sicurezza.

Esempi:

- Se i processi di manutenzione o riparazione non sono allineati con i requisiti aziendali, possono verificarsi tempi di inattività inaccettabili.
- Se i requisiti di sicurezza non vengono presi in considerazione al momento dell'acquisto delle tecnologie informatiche, può aumentare il rischio di attacchi ai sistemi informatici dell'azienda.
- Se i materiali di consumo necessari non vengono resi disponibili tempestivamente, i processi informatici che ne dipendono possono vacillare.
- Vulnerabilità possono sorgere se nella pianificazione di una procedura informatica si scelgono protocolli di trasmissione non adatti.

La tecnologia dell'informazione e l'intero ambiente di un ente pubblico o di un'azienda sono in continua evoluzione. Sia che i dipendenti lascino o entrino a far parte dell'azienda, sia che vengano acquistati nuovi hardware o software, sia che un'azienda fornitrice dichiari fallimento. Se i necessari adeguamenti organizzativi e tecnici non vengono presi in considerazione o lo sono solo in misura insufficiente, possono sorgere dei pericoli.

Esempi:

- A causa di modifiche strutturali nell'edificio, le vie di fuga esistenti vengono modificate. Poiché i dipendenti non sono stati sufficientemente informati, l'edificio non può essere evacuato nei tempi previsti.
- Quando si trasmettono documenti elettronici, non si fa attenzione a utilizzare un formato di dati leggibile per la parte ricevente.

G 0.19 Divulgazione di informazioni meritevoli di protezione

I dati e le informazioni riservate possono essere accessibili solo alle persone autorizzate a prenderne visione. Insieme all'integrità e alla disponibilità, la riservatezza è uno dei valori fondamentali della sicurezza delle informazioni. Per le informazioni riservate (come password, dati personali, segreti aziendali o ufficiali, dati di sviluppo), esiste il pericolo intrinseco di essere divulgate a causa di un guasto tecnico, di una disattenzione o anche di azioni deliberate. Queste informazioni riservate possono essere accessibili in diversi punti, ad esempio

- sui supporti di memorizzazione all'interno dei computer (dischi rigidi);
- su supporti di memorizzazione rimovibili (chiavette USB, CD o DVD);
- in forma stampata su carta (stampe, file);
- sui percorsi di trasmissione durante la trasmissione dei dati.

Anche il modo in cui le informazioni vengono divulgate può essere molto diverso, ad esempio:

- lettura non autorizzata di file,
- divulgazione incauta, ad esempio nel corso di ordini di riparazione;
- cancellazione o distruzione inadeguata dei supporti di dati;
- furto del supporto dati e successiva valutazione;
- intercettazione di linee di trasmissione;
- infezione dei sistemi informatici con malware;
- lettura sullo schermo o intercettazione di conversazioni.

La divulgazione di informazioni sensibili può avere gravi conseguenze per una organizzazione. Tra l'altro, la perdita di riservatezza può portare ai seguenti effetti negativi per una organizzazione:

- Violazione delle leggi, ad esempio in materia di protezione dei dati e di segreto bancario;
- Impatto interno negativo, ad esempio demoralizzazione dei dipendenti;
- Effetti esterni negativi, ad esempio compromissione delle relazioni con i partner commerciali, perdita di fiducia da parte dei clienti;
- Effetti finanziari, ad esempio richieste di risarcimento danni, multe, spese legali;

- compromissione del diritto all'autodeterminazione informativa.

Una perdita di riservatezza non sempre viene notata immediatamente. Spesso si scopre solo in un secondo momento, ad esempio attraverso le inchieste della stampa, che persone non autorizzate hanno avuto accesso a informazioni riservate.

Esempio:

- Gli acquirenti di computer, dischi rigidi, telefoni cellulari o dispositivi simili di seconda mano spesso vi trovano informazioni altamente riservate, come dati di persone malate o numeri di conto corrente.

G 0.20 Informazioni o prodotti da fonti inaffidabili

Se si utilizzano informazioni, software o dispositivi che provengono da fonti inaffidabili o la cui origine e correttezza non sono state adeguatamente verificate, l'utilizzo può comportare rischi elevati. Ciò può comportare, tra l'altro, che le informazioni rilevanti per l'azienda si basino su dati falsi, che i calcoli forniscono risultati errati o che si prendano decisioni sbagliate. Anche l'integrità e la disponibilità dei sistemi informatici possono essere compromesse.

Esempi:

- Una persona può essere indotta a compiere determinate azioni dannose per sé o per altri da e-mail di cui non ha controllato l'origine. Ad esempio, l'e-mail può contenere allegati o link interessanti che, se cliccati, portano all'installazione di malware. L'indirizzo del mittente dell'e-mail può essere falsificato o imitare quello di una persona (personalmente) nota.
- L'ipotesi che un'affermazione sia vera perché è "sul giornale" o "è stata trasmessa in TV" non è sempre giustificata. Di conseguenza, dichiarazioni false possono essere incorporate in rapporti critici nei confronti delle istituzioni.
- L'affidabilità delle informazioni diffuse via Internet varia notevolmente. Se le affermazioni vengono prese da Internet senza ulteriori controlli delle fonti, si possono prendere decisioni sbagliate.
- Se si applicano aggiornamenti o patch da fonti non affidabili, si possono verificare effetti collaterali indesiderati. Se non si controlla l'origine del software, aumenta il rischio che i sistemi informatici vengano infettati da codici dannosi.

G 0.21 Manipolazione di hardware e software

La manipolazione è una qualsiasi forma di intervento mirato ma clandestino per modificare inosservati oggetti di qualsiasi tipo. La manipolazione di hardware o software può essere effettuata, tra l'altro, per sentimenti di vendetta, per provocare volontariamente un danno, per ottenere vantaggi personali o per arricchimento. L'obiettivo può essere costituito da dispositivi di ogni tipo, accessori, supporti di dati (ad esempio DVD, chiavette USB), applicazioni, database o simili.

La manipolazione di hardware e software non sempre comporta un danno immediato. Tuttavia, se le informazioni elaborate con essi vengono compromesse, ciò può comportare impatti sulla sicurezza di ogni tipo (perdita di riservatezza, integrità o disponibilità). Le manipolazioni possono essere tanto più efficaci quanto più tardi vengono scoperte, quanto più ampia è la conoscenza degli attaccanti e quanto più profondo è l'impatto su un processo di lavoro. Gli effetti vanno dall'accesso non autorizzato a dati meritevoli di protezione fino alla distruzione di supporti dati o sistemi informatici. Le manipolazioni possono anche comportare notevoli tempi di inattività.

Esempi:

- In una società finanziaria svizzera, alcuni dipendenti avevano manipolato il software applicativo di alcuni servizi finanziari. Questo ha permesso loro di ottenere illegalmente quantità maggiori di denaro.
- Manipolando i bancomat, gli aggressori sono riusciti più volte a leggere illegalmente i dati memorizzati sulle carte di pagamento. In combinazione con i PIN spiati, questi dati sono stati successivamente utilizzati per prelevare denaro a spese dei titolari delle carte.

G 0.22 Manipolazione di informazioni

Le informazioni possono essere manipolate in molti modi, ad esempio attraverso l'inserimento di dati errati o deliberatamente falsi, la modifica del contenuto dei campi del database o della corrispondenza. In linea di principio, questo vale non solo per le informazioni digitali, ma anche per i documenti cartacei, ad esempio. Tuttavia, gli aggressori possono manipolare solo le informazioni a cui hanno accesso. Più diritti di accesso una persona ha ai file e alle directory dei sistemi IT o più accesso alle informazioni ha, più manipolazioni gravi può effettuare. Se le manipolazioni non vengono individuate tempestivamente, il regolare svolgimento dei processi aziendali e delle attività specialistiche può essere gravemente compromesso.

I documenti archiviati rappresentano solitamente informazioni che meritano di essere protette. La manipolazione di tali documenti è particolarmente grave, poiché può essere notata solo dopo anni e la verifica spesso non è più possibile.

Esempio:

- Un'impiegata era talmente infastidita dalla promozione del suo collega nel reparto contabilità che ha ottenuto l'accesso non autorizzato al computer del collega durante una breve assenza. In questo caso ha avuto un'enorme influenza negativa sul risultato annuale pubblicato dell'azienda, modificando alcune cifre del bilancio mensile.

G 0.23 Intrusione non autorizzata nei sistemi informatici

In linea di principio, ogni interfaccia di un sistema informatico non comprende solo la possibilità di utilizzo autorizzato di determinati servizi del sistema informatico, ma anche il rischio di accesso non autorizzato al sistema informatico.

Esempi:

- Se i dati di accesso vengono spiati, è ipotizzabile un uso non autorizzato delle applicazioni o dei sistemi IT protetti con essi.
- Gli aggressori potrebbero ottenere un accesso non autorizzato ai sistemi IT tramite un accesso di manutenzione remota non adeguatamente protetto.
- Nel caso di interfacce non adeguatamente protette di componenti di rete attivi, è ipotizzabile che gli aggressori possano ottenere un accesso non autorizzato al componente di rete. Se riescono anche a superare i meccanismi di sicurezza locali, ad esempio ottenendo le autorizzazioni amministrative, possono eseguire tutte le attività amministrative.
- Molti sistemi IT dispongono di interfacce per l'utilizzo di dispositivi di archiviazione dati intercambiabili, come schede di memoria aggiuntive o supporti di archiviazione USB. Se un sistema informatico con il relativo hardware e software viene lasciato incustodito, c'è il rischio di leggere grandi quantità di dati senza autorizzazione o di introdurre malware.

G 0.24 Distruzione di apparecchiature o supporti dati

La negligenza, l'uso improprio, ma anche una gestione non qualificata possono portare alla distruzione dei dispositivi e dei supporti di dati, che possono interrompere gravemente il funzionamento del sistema IT.

C'è anche il rischio di perdere informazioni importanti a causa della distruzione, che non possono essere ricostruite o possono essere ricostruite solo con grande sforzo.

Esempi:

- In un'azienda, una persona interna ha sfruttato la sua conoscenza del fatto che un server importante era sensibile alle temperature di esercizio eccessive e ha bloccato le fessure di ventilazione per la ventola dell'alimentatore con un oggetto nascosto dietro il server. Due giorni dopo, il disco rigido del server ha subito un difetto legato alla temperatura e il server si è guastato per diversi giorni.
- Un dipendente si era talmente arrabbiato per i ripetuti crash del sistema che ha sfogato la sua rabbia sulla sua workstation. Nel processo, il disco rigido è stato così gravemente danneggiato dai calci al computer che è diventato inutilizzabile. I dati memorizzati poterono essere ricostruiti solo in parte grazie a un backup del giorno precedente.
- I cortocircuiti possono essere causati in un sistema IT anche da tazze di caffè rovesciate o dall'umidità che penetra quando si annaffiano i fiori.

G 0.25 Guasto di apparecchiature o sistemi

Se le applicazioni critiche dal punto di vista temporale sono gestite da un sistema IT, i danni conseguenti a un guasto del sistema sono elevati, se non esistono opzioni di fallback.

Esempi:

- In un sistema IT viene installato un firmware non previsto per questo tipo di sistema. Il sistema IT non si avvia più senza errori e deve essere reso nuovamente operativo dal produttore.
- Presso un Internet Service Provider (ISP), un errore di alimentazione in un sistema di archiviazione ne ha causato l'arresto. Sebbene il guasto vero e proprio sia stato eliminato rapidamente, i sistemi IT interessati non potevano essere riavviati in seguito a causa di incongruenze nel file system. Di conseguenza, diversi server web gestiti dall'ISP non sono stati accessibili per giorni.

G 0.26 Malfunzionamento di apparecchiature o sistemi

Oggi, i dispositivi e i sistemi che servono all'elaborazione delle informazioni hanno spesso molte funzioni e sono quindi strutturati in modo complesso. Fondamentalmente, questo riguarda sia i componenti hardware che quelli software. A causa della complessità, ci sono molte fonti di errore in questi componenti. Di conseguenza, i dispositivi e i sistemi falliscono ripetutamente nel funzionare come previsto, causando problemi di sicurezza.

Le cause dei malfunzionamenti sono molteplici, ad esempio l'affaticamento dei materiali, le tolleranze di fabbricazione, le debolezze concettuali, il superamento dei valori limite, le condizioni operative non previste o la mancanza di manutenzione. Poiché non esistono dispositivi e sistemi perfetti, una certa probabilità residua di malfunzionamento deve essere sempre accettata.

Tutti i valori fondamentali della sicurezza delle informazioni (riservatezza, integrità, disponibilità) possono essere compromessi da malfunzionamenti di dispositivi o sistemi. Inoltre, i malfunzionamenti possono rimanere inosservati per un periodo di tempo lungo. Di conseguenza, può accadere, ad esempio, che i risultati dei calcoli vengano falsificati e non corretti in tempo.

Esempi:

- A causa di una griglia di ventilazione bloccata, un sistema di archiviazione si surriscalda e non si guasta completamente, ma presenta solo malfunzionamenti sporadici. Solo alcune settimane dopo si nota che le informazioni memorizzate sono incomplete.
- Un'applicazione scientifica standard viene utilizzata per eseguire un'analisi statistica su un set di dati pre-collocati e archiviati in un database. Tuttavia, secondo la documentazione, l'applicazione non è stata rilasciata per il prodotto di database utilizzato. L'analisi sembra funzionare, ma i controlli casuali mostrano che i risultati calcolati sono sbagliati. I problemi di compatibilità tra l'applicazione e il database sono stati identificati come la causa.

G 0.27 Mancanza di risorse

Se le risorse disponibili in un'area sono insufficienti, ciò può portare a colli di bottiglia nella fornitura di tali risorse e persino a sovraccarichi e guasti. A seconda del tipo di risorse interessate, un piccolo evento, il cui verificarsi era anche prevedibile, può in ultima analisi influenzare un gran numero di processi aziendali. Le carenze di risorse possono verificarsi nelle operazioni informatiche e nei collegamenti di comunicazione, ma anche in altre aree di un'organizzazione. Se le risorse umane, temporali e finanziarie disponibili per determinati compiti sono insufficienti, ciò può avere una serie di effetti negativi. Può accadere, ad esempio, che i ruoli necessari per i progetti non siano ricoperti da persone adeguate. Se le risorse operative, come l'hardware o il software, non sono più sufficienti a soddisfare i requisiti, i compiti specializzati potrebbero non essere eseguiti con successo.

Spesso le carenze in termini di personale, tempo, finanze, tecnologia e altri fattori possono essere compensate durante le operazioni regolari per un periodo di tempo limitato. In condizioni di forte pressione temporale, invece, diventano ancora più evidenti, ad esempio in situazioni di emergenza.

Le risorse possono anche essere deliberatamente sovraccaricate se qualcuno genera intenzionalmente una domanda intensiva di una risorsa e quindi provoca un'interruzione intensiva e permanente della risorsa, vedi anche G 0.40 Denial of service.

Esempi:

- I cavi elettrici sovraccarichi si riscaldano e, se non sono posati correttamente, possono provocare un incendio.
- Se sulla rete vengono utilizzate nuove applicazioni con un requisito di larghezza di banda superiore a quello considerato al momento della pianificazione, ciò può portare a una perdita di disponibilità dell'intera rete se l'infrastruttura di rete non può essere scalata a sufficienza.
- Se gli operatori controllano solo sporadicamente i file di log dell'IT che supportano a causa del sovraccarico, gli attacchi potrebbero non essere rilevati tempestivamente.
- I server web possono essere talmente sovraccaricati da un elevato volume di richieste che arrivano contemporaneamente che l'accesso regolare ai dati diventa quasi impossibile.
- Se un'azienda è sottoposta a una procedura di insolvenza, potrebbero mancare i soldi per i pezzi di ricambio urgenti o i fornitori di servizi importanti potrebbero non essere pagati.

G 0.28 Errori o punti deboli di software

Per qualsiasi software, quanto più è complesso, tanto più frequentemente si verificano errori. Anche con test intensivi, di solito non tutti gli errori vengono scoperti prima della consegna ai clienti. Se gli errori del software non vengono rilevati in tempo, i crash o gli errori che si verificano durante l'uso possono portare a conseguenze di vasta portata. Ad esempio, risultati di calcolo errati, decisioni sbagliate da parte del management della organizzazione e ritardi nei processi aziendali.

Le vulnerabilità o gli errori del software possono causare gravi lacune nella sicurezza di un'applicazione, di un sistema informatico o di tutti i sistemi informatici collegati in rete con esso. In determinate circostanze, tali lacune di sicurezza possono essere sfruttate da malintenzionati per introdurre malware, leggere dati senza autorizzazione o effettuare manipolazioni.

Esempi:

- La maggior parte degli allarmi emessi dai Computer Emergency Response Teams (CERT) negli ultimi anni riguarda errori di programmazione legati alla sicurezza. Si tratta di errori che si verificano durante la creazione di un software e che portano a un uso improprio dello stesso. Gran parte di questi errori sono stati causati da overflow di memoria (buffer overflow).
- I browser Internet sono oggi un componente software importante sui client. I browser sono spesso utilizzati non solo per accedere a Internet, ma anche per le applicazioni Web interne di aziende e autorità pubbliche. Le vulnerabilità o gli errori del software nei browser possono quindi avere un impatto particolarmente forte sulla sicurezza informatica nel suo complesso.

G 0.29 Violazione di leggi o regolamenti

Se le informazioni, i processi aziendali e i sistemi informatici di un istituto non sono adeguatamente protetti (ad esempio, a causa di una gestione inadeguata della sicurezza), ciò può portare a violazioni della legislazione relativa al trattamento delle informazioni o dei contratti esistenti con i partner commerciali. Le leggi da osservare in ciascun caso dipendono dalla natura dell'istituzione o dei suoi processi e servizi aziendali. A seconda del luogo in cui si trovano le sedi di un'istituzione, è possibile che debbano essere rispettate anche normative nazionali diverse. I seguenti esempi illustrano questo aspetto:

- In Germania, il trattamento dei dati personali è regolato da una moltitudine di norme. Tra queste, la legge federale sulla protezione dei dati e le leggi statali sulla protezione dei dati, ma anche una moltitudine di normative specifiche per ogni area.
- La direzione di un'azienda ha l'obbligo di esercitare una ragionevole attenzione in tutti i processi aziendali. Ciò include l'osservanza delle misure di sicurezza riconosciute. In Germania sono in vigore diverse norme giuridiche, come la KonTraG (Legge sul controllo e la trasparenza negli affari), la GmbHG (Legge sulle società a responsabilità limitata) o la AktG (Legge sulle società per azioni), da cui si possono dedurre i corrispondenti obblighi di azione e responsabilità della direzione o del consiglio direttivo di una società in materia di gestione del rischio e sicurezza delle informazioni.
- Il corretto trattamento dei dati contabili è disciplinato da diverse leggi e regolamenti. In Germania, queste includono il Codice commerciale tedesco (ad esempio, HGB §§ 238 e seguenti) e il Codice fiscale tedesco (AO). Il corretto trattamento delle informazioni include naturalmente il loro trattamento sicuro. In molti Paesi, entrambe le cose devono essere verificate regolarmente, ad esempio dai revisori dei conti nell'ambito della revisione del bilancio annuale. Se vengono riscontrate gravi carenze nella sicurezza, non è possibile emettere un rapporto di audit positivo.
- In molti settori (ad esempio l'industria automobilistica) è prassi comune che le aziende produttrici obblighino i propri fornitori a rispettare determinati standard di qualità e sicurezza. In questo contesto, vengono sempre più spesso imposti anche requisiti di sicurezza delle informazioni. Se un partner contrattuale vìola i requisiti di sicurezza previsti dal contratto, ciò può comportare sanzioni contrattuali, ma anche la risoluzione dei contratti o addirittura la perdita dei rapporti commerciali.

Solo pochi requisiti di sicurezza derivano direttamente dalla legislazione. Tuttavia, la legislazione è generalmente guidata dallo stato dell'arte come base di valutazione generale per il grado di sicurezza raggiungibile. Se le misure di sicurezza esistenti in una

organizzazione non sono proporzionate ai valori da proteggere e allo stato dell'arte, ciò può avere gravi conseguenze.

G 0.30 Utilizzo o amministrazione non autorizzata di apparecchiature e sistemi

Senza meccanismi adeguati per il controllo degli ingressi ed accessi, l'uso non autorizzato di dispositivi e sistemi non può praticamente essere impedito o rilevato. Per i sistemi informatici, il meccanismo di base è l'identificazione e l'autenticazione degli utenti. Tuttavia, anche nel caso di sistemi IT con una capacità di identificazione e autenticazione forte, l'uso non autorizzato è concepibile se le caratteristiche di sicurezza corrispondenti (password, smart card, token, ecc.) cadono nelle mani sbagliate. Anche nell'assegnazione e nel mantenimento delle autorizzazioni si possono commettere molti errori, ad esempio se le autorizzazioni vengono assegnate in modo troppo ampio o a persone non autorizzate o non vengono aggiornate tempestivamente.

Le persone non autorizzate possono ottenere informazioni riservate, effettuare manipolazioni o causare interruzioni attraverso l'uso non autorizzato di dispositivi e sistemi.

Un caso particolare di utilizzo non autorizzato è l'amministrazione non autorizzata. Se persone non autorizzate modificano la configurazione o i parametri di funzionamento dei componenti hardware o software, possono verificarsi gravi danni.

Esempio:

- Durante il controllo dei dati di registrazione, gli operatori IT si sono imbattuti in eventi inizialmente inspiegabili che si verificavano in giorni diversi, ma frequentemente al mattino presto e nel pomeriggio. Da un'indagine più approfondita è emerso che un router WLAN era configurato in modo insicuro. Le persone in attesa alla fermata dell'autobus di fronte all'edificio aziendale utilizzavano questo accesso per navigare in Internet con i loro dispositivi mobili durante l'attesa.

G 0.31 Uso o amministrazione errata di apparecchiature e sistemi

Un uso scorretto o improprio di apparecchiature, sistemi e applicazioni può comprometterne la sicurezza, soprattutto se le misure di sicurezza esistenti vengono ignorate o aggirate. Questo spesso porta a malfunzionamenti o guasti. Tuttavia, a seconda dei tipi di dispositivi o sistemi utilizzati in modo scorretto, possono essere violate anche la riservatezza e l'integrità delle informazioni.

Un caso speciale particolarmente importante di uso scorretto è l'amministrazione scorretta. Gli errori nell'installazione, nella configurazione, nella manutenzione e nella cura dei componenti hardware o software possono causare gravi danni.

Ad esempio, diritti assegnati in modo troppo generoso, password facili da indovinare, supporti di dati con copie di backup non sufficientemente protetti o terminali non bloccati durante le assenze temporanee possono causare incidenti di sicurezza.

Allo stesso modo, i dati possono essere cancellati o modificati accidentalmente a causa di un funzionamento non corretto dei sistemi o delle applicazioni informatiche. Questo potrebbe anche portare a rendere pubbliche informazioni riservate, ad esempio se i diritti di accesso sono impostati in modo errato.

Se i cavi di alimentazione o di rete sono posati senza protezione, possono essere danneggiati involontariamente, causando il malfunzionamento dei collegamenti. I cavi di collegamento dei dispositivi possono essere strappati se le persone vi inciampano.

G 0.32 Uso improprio delle autorizzazioni

A seconda dei loro ruoli e compiti, le persone ricevono le corrispondenti autorizzazioni di ingresso, accesso e uso. In questo modo, da un lato si gestisce e controlla l'accesso alle informazioni, dall'altro si abilitano le persone a svolgere determinati compiti. Ad esempio, le persone o i gruppi hanno bisogno di determinate autorizzazioni per poter eseguire applicazioni o modificare informazioni.

L'uso improprio delle autorizzazioni si verifica quando le possibilità acquisite legalmente o illegalmente vengono intenzionalmente utilizzate al di fuori del contesto previsto. L'obiettivo è spesso quello di ottenere vantaggi personali o di danneggiare un'istituzione o determinate persone.

In non pochi casi, per motivi storici, legati al sistema o di altro tipo le persone dispongono di diritti di accesso più elevati o più ampi di quelli necessari per le loro attività. In determinate circostanze, questi diritti possono essere utilizzati in modo improprio per compiere attacchi.

Esempi:

- Più i diritti di accesso alle informazioni sono finemente granulari, più spesso è necessario uno sforzo di manutenzione per mantenere aggiornate queste autorizzazioni. C'è quindi il rischio di differenziare troppo poco i vari ruoli nell'assegnazione dei diritti di accesso, rendendo più facile l'uso improprio delle autorizzazioni.
- In diverse applicazioni, le autorizzazioni di accesso o le password sono memorizzate in aree del sistema accessibili anche ad altri utenti. Questo potrebbe consentire agli aggressori di modificare le autorizzazioni o leggere le password.
- Chi dispone di autorizzazioni troppo generose potrebbe essere tentato di accedere ai file altrui, ad esempio per visualizzare la posta elettronica di un'altra persona perché ha bisogno di determinate informazioni con urgenza.

G 0.33 Mancanza di personale

La perdita di personale può avere un impatto significativo su un'istituzione e sui suoi processi aziendali. Il personale può assentarsi in modo imprevedibile a causa di malattia, infortunio, morte o sciopero, ad esempio. Inoltre, si deve tenere conto anche della prevedibile perdita di personale in caso di congedo, formazione continua o regolare cessazione del rapporto di lavoro, soprattutto se l'orario di lavoro rimanente è ridotto, ad esempio a causa di un diritto alle ferie. Una perdita di personale può anche essere causata da un cambio di lavoro interno.

Esempi:

- A causa di una malattia prolungata, la persona responsabile dell'amministrazione della rete di un'azienda era assente dal servizio. Nell'azienda in questione, la rete inizialmente ha continuato a funzionare senza errori. Tuttavia, dopo due settimane, a seguito di un crash del sistema, nessuno è stato in grado di risolvere l'errore perché c'era solo questo dipendente addestrato al funzionamento della rete. Questo ha portato a un'interruzione della rete per diversi giorni.
- Durante il congedo di un membro del personale delle operazioni IT, un istituto ha dovuto ricorrere ai supporti di backup nella cassaforte di salvataggio dei dati. Il codice di accesso alla cassaforte era stato cambiato poco tempo prima ed era noto solo a questo dipendente. Il ripristino dei dati ha potuto essere effettuato solo dopo diversi giorni, perché il dipendente non era disponibile prima, essendo in vacanza.
- In caso di pandemia, sempre più personale diventa gradualmente indisponibile per periodi di tempo più lunghi, a causa della malattia stessa, della necessaria assistenza ai parenti o della cura dei bambini. Alcuni membri del personale rimangono anche fuori servizio per paura di un'infezione sui mezzi di trasporto pubblico o all'interno dell'istituto. Di conseguenza, è possibile svolgere solo il lavoro più necessario. La manutenzione necessaria dei sistemi, che si tratti del server centrale o dell'aria condizionata nel centro informatico, non può più essere effettuata. Di conseguenza, sempre più sistemi si guastano.

G 0.34 Attacchi

Un attacco può minacciare una organizzazione, aree specifiche dell'organizzazione o singoli individui. Le possibilità tecniche per compiere un attacco sono molteplici: lancio di mattoni, uso di esplosivi, uso di armi da fuoco, incendio doloso. Se e in che misura una organizzazione è esposta al pericolo di un attacco dipende fortemente dai suoi compiti e dal clima politico-sociale, oltre che dalla posizione e dall'ambiente dell'edificio. Le aziende e le autorità che operano in aree politicamente controverse sono più minacciate di altre. Le organizzazioni che si trovano in prossimità di aree dimostrative comuni sono più a rischio di quelle che si trovano in località remote. Per la valutazione della minaccia o in caso di sospetto in Germania, gli Uffici Statali di Polizia Criminale o l'Ufficio Federale di Polizia Criminale (Bundeskriminalamt) possono fornire consulenza sulla valutazione della minaccia o in caso di sospetto di un attacco a sfondo politico. L'Ufficio Federale di Polizia Criminale può essere consultato per una consulenza.

Esempi:

- Negli anni '80 fu effettuato un attacco esplosivo al centro informatico di una grande autorità federale a Colonia. L'elevato impatto dell'ordigno esplosivo distrusse non solo le finestre e le pareti, ma anche molti sistemi informatici del centro informatico.
- L'attacco al World Trade Center di New York dell'11 settembre 2001 non solo ha ucciso molte persone, ma ha anche distrutto numerose strutture informatiche. Di conseguenza, diverse aziende hanno avuto notevoli difficoltà a proseguire le loro attività commerciali.

G 0.35 Coercizione, estorsione o corruzione

La coercizione, l'estorsione o la corruzione possono portare alla compromissione della sicurezza delle informazioni o dei processi aziendali. Ad esempio, minacciando violenza o altri danni, un aggressore può cercare di convincere la vittima a disobbedire alle politiche di sicurezza o ad aggirare le misure di sicurezza (coercizione).

Invece di minacciare, gli aggressori possono anche offrire deliberatamente denaro o altri vantaggi per far sì che i dipendenti o altre persone siano lo strumento delle violazioni della sicurezza (corruzione). Ad esempio, c'è il rischio che i dipendenti corrotti passino documenti riservati a persone non autorizzate.

La coercizione o la corruzione possono, in linea di principio, compromettere tutti i valori fondamentali della sicurezza delle informazioni. Gli attacchi possono essere finalizzati, tra l'altro, a trasmettere informazioni riservate a persone non autorizzate, a manipolare informazioni critiche per l'azienda o a interrompere il regolare svolgimento dei processi aziendali.

Il pericolo è particolarmente elevato quando tali attacchi sono rivolti a dirigenti di alto livello o a persone che ricoprono particolari posizioni di fiducia.

G 0.36 Furto d'identità

Nel furto d'identità, gli aggressori fingono di avere una falsa identità, ossia utilizzano informazioni su un'altra persona per apparire a suo nome. A tal fine, vengono utilizzati informazioni come la data di nascita, l'indirizzo, i numeri di carta di credito o di conto, ad esempio per registrarsi presso un Internet Service Provider (ISP) a spese di qualcun altro o per arricchirsi in altro modo. Il furto d'identità spesso comporta anche, direttamente o indirettamente, un danno alla reputazione, ma comporta anche una grande quantità di tempo da dedicare a chiarire le cause e ad evitare conseguenze negative per le persone interessate. Alcune forme di frode d'identità vengono anche definite "mascherate".

Il furto d'identità è particolarmente comune quando la verifica dell'identità è troppo permissiva, soprattutto quando su di essa si basano servizi costosi.

Una persona che è stata ingannata sull'identità dell'altra persona può essere facilmente indotta a rivelare informazioni sensibili.

Esempi:

- Con i vari provider di e-mail e le piattaforme di aste su Internet, inizialmente era sufficiente inventare un nome immaginario e associarlo ad un indirizzo adeguato dall'elenco telefonico per registrarsi. All'inizio, gli aggressori potevano anche registrarsi con nomi inventati riconoscibili, ad esempio di personaggi dei fumetti. Quando sono stati introdotti test di plausibilità più severi, sono stati utilizzati anche nomi, indirizzi e numeri di conto di persone reali. Gli interessati lo hanno scoperto solo quando hanno ricevuto le prime richieste di pagamento.
- Gli indirizzi delle e-mail sono facili da falsificare. Capita spesso che gli utenti vengano ingannati e che pensino che un'e-mail provenga da una persona affidabile. Attacchi simili sono possibili manipolando l'ID del chiamante per le connessioni vocali o manipolando l'ID del fax per le connessioni fax.
- Gli aggressori possono utilizzare un mascheramento per cercare di connettersi a una connessione esistente senza doversi autenticare, in quanto questa fase è già stata eseguita dai partecipanti originali alla comunicazione.

G 0.37 Diniego di azioni

Le persone possono negare di aver commesso determinati atti per vari motivi, ad esempio perché questi atti violano istruzioni, requisiti di sicurezza o addirittura leggi. Ma possono anche negare di aver ricevuto una notifica, ad esempio perché hanno dimenticato un appuntamento. Nel campo della sicurezza informatica, quindi, viene spesso enfatizzata la non ripudiabilità, una proprietà volta a garantire che le azioni compiute non possano essere negate senza giustificazione. Nel mondo anglosassone si usa il termine non-repudiation.

Nel caso della comunicazione, si fa un'ulteriore distinzione tra i partecipanti alla comunicazione che negano la ricezione di un messaggio (ripudio della ricezione) e l'invio di un messaggio (ripudio dell'origine). La negazione della ricezione dei messaggi può essere importante nelle transazioni finanziarie, ad esempio se qualcuno nega di aver ricevuto una fattura in tempo. Può anche accadere che i partecipanti alla comunicazione neghino l'invio di messaggi, ad esempio negando che un ordine sia stato effettuato. L'invio o la ricezione di messaggi può essere negata tanto quando si spedisce per posta quanto quando si usa il fax o la posta elettronica.

Esempio:

- Un pezzo di ricambio urgente viene ordinato per via elettronica. Dopo una settimana viene presentato un reclamo per il pezzo mancante; nel frattempo sono stati sostenuti costi elevati a causa della perdita di produzione. L'azienda fornitrice nega di aver ricevuto l'ordine.

G 0.38 Uso improprio di dati personali

I dati personali sono quasi sempre informazioni che richiedono una protezione speciale. Esempi tipici sono le informazioni su circostanze personali o fattuali di una persona fisica identificata o identificabile. Se la protezione dei dati personali non è adeguatamente garantita, c'è il rischio che le persone interessate siano danneggiate nella loro posizione sociale o nella loro situazione economica.

L'uso improprio dei dati personali può verificarsi, ad esempio, se un'istituzione raccoglie un numero eccessivo di dati personali, li ha raccolti senza una base legale o un consenso, li utilizza per uno scopo diverso da quello consentito al momento della raccolta, li cancella troppo tardi o li trasmette senza autorizzazione.

Esempi:

- I dati personali possono essere trattati solo per lo scopo per cui sono stati raccolti o memorizzati per la prima volta. È pertanto inammissibile l'uso di file di log, in cui vengono registrati i login e i logout degli utenti ai sistemi informatici esclusivamente per il controllo degli accessi da utilizzare come controllo della presenza e del comportamento.
- Le persone che hanno accesso ai dati personali potrebbero trasmetterli senza autorizzazione. Ad esempio, il personale della reception di un hotel potrebbe vendere i dati di accesso degli ospiti a società pubblicitarie.

G 0.39 Malware

Un programma dannoso (malware) è un software sviluppato con lo scopo di eseguire funzioni indesiderate e solitamente dannose. I tipi tipici di malware includono virus, worm e cavalli di Troia. I programmi dannosi si attivano di solito di nascosto, senza che l'utente ne sia a conoscenza o abbia dato il suo consenso.

Oggi il malware offre agli aggressori ampie possibilità di comunicazione e controllo e possiede una moltitudine di funzioni. Tra le altre cose, il malware può indagare in modo specifico sulle password, controllare i sistemi da remoto, disattivare il software di protezione e spiare i dati.

La perdita o la falsificazione di informazioni o applicazioni è particolarmente importante come danno. Tuttavia, anche la perdita di immagine e i danni finanziari che possono essere causati dal malware sono di grande importanza.

Esempi:

- In passato, il malware W32/Bugbear si diffondeva in due modi: cercava nelle reti locali i computer con condivisioni a cui era possibile accedere in scrittura e si copiava su di essi. Inoltre, si inviava come e-mail HTML agli indirizzi di posta elettronica presenti nella rubrica dei computer infetti. A causa di una falla nella routine HTML di alcuni programmi di posta elettronica, il malware veniva eseguito all'apertura del messaggio senza alcuna ulteriore azione da parte del destinatario.
- -l malware W32/Klez si è diffuso in diverse varianti. I computer infetti inviavano il virus a tutti gli indirizzi e-mail presenti nella rubrica del computer. Una volta che il virus ha infettato un computer, impedisce l'installazione di programmi antivirus manipolando continuamente il sistema operativo, rendendo così molto più difficile la disinfezione dei computer infetti.

G 0.40 Denial of Service

Esistono diverse forme di attacco che mirano a impedire l'uso previsto di determinati servizi, funzioni o dispositivi. Il termine generico per tali attacchi è "Denial of Service". Si usa spesso anche il termine "attacco DoS". Tali attacchi possono provenire, tra l'altro, da dipendenti scontenti, clienti o aziende concorrenti. Ma anche ricatti o motivi politici possono essere alla base di questi attacchi. L'obiettivo degli attacchi può essere costituito da valori rilevanti per l'azienda di qualsiasi tipo. Le manifestazioni tipiche degli attacchi DoS sono:

- Interruzione dei processi aziendali, ad esempio inondando l'accettazione degli ordini con ordini errati;
- compromissione dell'infrastruttura, ad esempio bloccando le porte dell'istituto;
- causare guasti informatici, ad esempio sovraccaricando deliberatamente i servizi di un server della rete.

Questo tipo di attacco è spesso legato alle risorse distribuite, nel senso che queste risorse vengono talmente richieste ed utilizzate da non essere più disponibili per gli utenti effettivi. Negli attacchi basati sull'IT, ad esempio, le seguenti risorse possono essere artificialmente scarse: Processi, tempo CPU, memoria, spazio su disco, capacità di trasmissione.

Esempio:

- Nella primavera del 2007 si sono verificati forti attacchi DoS su numerose offerte Internet in Estonia per un lungo periodo di tempo. Ciò ha comportato una notevole riduzione dell'utilizzo di informazioni e servizi su Internet in Estonia.

G 0.41 Sabotaggio

Per sabotaggio si intende la manipolazione o il danneggiamento intenzionale di oggetti o processi con l'obiettivo di danneggiare la vittima. I centri dati o i collegamenti di comunicazione di autorità o aziende possono essere obiettivi particolarmente attraenti, in quanto è possibile ottenere un grande effetto con mezzi relativamente piccoli.

La complessa infrastruttura di un data center può essere manipolata in modo selettivo influenzando deliberatamente componenti importanti, eventualmente da autori esterni, ma soprattutto interni, al fine di causare interruzioni operative. Particolarmente a rischio sono le infrastrutture tecniche di edificio o di comunicazione non adeguatamente protette, nonché i punti di approvvigionamento centrali che possono non essere monitorati da un punto di vista organizzativo o tecnico e sono facilmente e inosservabilmente accessibili a soggetti esterni.

Esempi:

- In un grande centro dati, la manipolazione dell'UPS ha portato a un guasto totale temporaneo. Ciò ha comportato la ripetuta commutazione manuale dell'UPS in bypass e la successiva manipolazione dell'alimentazione principale dell'edificio. In totale si sono verificati quattro guasti in tre anni. In alcuni casi si sono verificati anche danni all'hardware. Le interruzioni del servizio duravano tra i 40 e i 130 minuti.
- Anche le strutture sanitarie erano ospitate all'interno di un centro dati. Bloccando gli scarichi e aprendo contemporaneamente la rete idrica, l'acqua è penetrata nei componenti tecnici centrali. I danni così provocati hanno causato interruzioni nel funzionamento del sistema produttivo.
- Il sabotaggio rappresenta un rischio particolare per gli archivi elettronici, poiché molti documenti meritevoli di protezione sono solitamente conservati in uno spazio ridotto. In determinate circostanze, questo può causare molti danni attraverso manipolazioni mirate e a basso sforzo.

G 0.42 Social engineering

L'ingegneria sociale (social engineering) è un metodo per ottenere un accesso non autorizzato alle informazioni o ai sistemi IT attraverso azioni sociali. L'ingegneria sociale sfrutta le caratteristiche umane come la disponibilità, la fiducia, la paura o il rispetto per l'autorità. In questo modo, i dipendenti possono essere manipolati per agire in modo improprio. Un caso tipico di attacchi con l'aiuto dell'ingegneria sociale è la manipolazione dei dipendenti tramite telefonate, in cui gli aggressori fingono di essere, ad esempio:

- una persona del front office il cui responsabile vuole fare qualcosa velocemente, ma ha dimenticato la sua password e ora ne ha urgentemente bisogno;
- una persona del reparto IT che chiama per un errore di sistema per il quale è ancora necessaria la password per correggere l'errore.

Quando arrivano le domande critiche, la persona curiosa è presumibilmente "solo un precario" o una persona "importante".

Un'altra strategia di ingegneria sociale sistematica consiste nel costruire una relazione più lunga con la vittima. Facendo molte telefonate non importanti in anticipo, gli aggressori possono raccogliere conoscenze e costruire una fiducia che può essere sfruttata in seguito.

Tali attacchi possono anche essere multi-stadio, costruendo ulteriori fasi sulla base delle conoscenze e delle tecniche acquisite nelle fasi precedenti.

Molti utenti sanno che non devono dare le password a nessuno. Gli ingegneri sociali lo sanno e quindi devono utilizzare altri mezzi per raggiungere l'obiettivo desiderato. Alcuni esempi sono:

- Gli aggressori possono chiedere alla vittima di eseguire comandi o applicazioni a loro sconosciuti, ad esempio perché si tratta di aiutare a risolvere un problema informatico. Può trattarsi di un'istruzione nascosta per modificare i diritti di accesso. In questo modo gli aggressori possono ottenere informazioni sensibili.
- Molti utenti utilizzano password forti, ma sono utilizzate per più account. Se gli aggressori gestiscono un servizio di rete utile (come un sistema di indirizzi e-mail) che richiede l'autenticazione degli utenti, possono ottenere le password e i login desiderati. Molti utenti utilizzeranno le credenziali che usano per questo servizio anche per altri servizi.

Quando gli aggressori ottengono password o altre funzioni di autenticazione senza autorizzazione, ad esempio con l'aiuto dell'ingegneria sociale, spesso si parla anche di "phishing" (composto da "password" e "fishing").

Nell'ingegneria sociale, gli aggressori non appaiono sempre in modo visibile. Spesso la vittima non scopre mai di essere stata sfruttata. Se questo ha successo, gli aggressori non devono aspettarsi di essere perseguiti e hanno anche una fonte per ottenere ulteriori informazioni in seguito.

G 0.43 Manipolazione di messaggi

In questa forma di attacco, gli aggressori inviano messaggi appositamente preparati a sistemi o persone con l'obiettivo di ottenere un vantaggio per sé o un danno per la vittima. Per costruire i messaggi in modo appropriato, si utilizzano, ad esempio, descrizioni di interfacce, specifiche di protocollo o registrazioni di comportamenti di comunicazione passati.

Esistono due casi speciali di manipolazione di messaggi che sono importanti nella pratica:

- In un "attacco replay" (riproduzione di messaggi), i messaggi validi vengono registrati e riprodotti (quasi) invariati in un momento successivo. Può anche essere sufficiente utilizzare solo parti di un messaggio, ad esempio una password, per ottenere un accesso non autorizzato a un sistema informatico.
- In un attacco "man-in-the-middle", gli aggressori assumono una posizione di mediazione inosservata nella comunicazione tra diversi partecipanti. Di norma, il mittente di un messaggio si finge il vero destinatario. Successivamente, l'unità ricevente finge di essere l'effettiva unità mittente. Se ciò riesce, gli aggressori possono ricevere messaggi non destinati a loro e valutarli e manipolarli prima che vengano inoltrati all'unità ricevente effettiva.

La crittografia delle comunicazioni non fornisce protezione contro gli attacchi man-in-the-middle se non c'è un'autenticazione sicura di coloro che partecipano alla comunicazione.

Esempi:

- Gli aggressori registrano i dati di autenticazione (ad esempio, nome dell'account e password) durante il processo di login dell'utente e utilizzano queste informazioni per accedere a un sistema. Nel caso di protocolli di autenticazione puramente statici, anche una password criptata può essere utilizzata per ottenere un accesso non autorizzato a un sistema di terzi.
- Per causare un danno economico all'azienda, i dipendenti effettuano più volte un ordine autorizzato.

G 0.44 Ingresso non autorizzato

L'ingresso di persone non autorizzate in un edificio o in singoli locali può comportare diversi altri pericoli. Questi includono, ad esempio, il furto o la manipolazione delle informazioni o dei sistemi IT. Nel caso di attacchi qualificati, il fattore decisivo è la durata del tempo in cui gli aggressori possono perseguire il loro obiettivo indisturbati.

Spesso, gli aggressori vogliono rubare componenti IT di valore o altri beni che possono essere facilmente venduti. Tuttavia, l'obiettivo di un'intrusione può anche essere quello di ottenere informazioni riservate, effettuare manipolazioni o interrompere i processi aziendali, tra le altre cose.

L'ingresso non autorizzato nei locali può quindi causare diversi tipi di danni:

- I danni alla proprietà possono verificarsi già a causa dell'ingresso non autorizzato stesso: le finestre e le porte vengono aperte con la forza e danneggiate nel processo e devono essere riparate o sostituite.
- Le apparecchiature o i componenti rubati, danneggiati o distrutti devono essere riparati o sostituiti.
- Possono verificarsi danni a causa della violazione della riservatezza, dell'integrità o della disponibilità delle informazioni o delle applicazioni.

Esempi:

- Vandalismo
- Durante un'irruzione in un'azienda durante il fine settimana, sono stati causati solo danni minori, forzando una finestra; sono stati rubati solo una cassa per il caffè e piccoli oggetti di arredamento. Durante un controllo di routine, tuttavia, si è poi scoperto che un server centrale era stato abilmente manipolato durante l'effrazione.

G 0.45 Perdita di dati

Per perdita di dati si intende un evento che impedisce l'utilizzo di uno stock di dati come richiesto (perdita di disponibilità). Una forma comune di perdita di dati si verifica quando questi vengono cancellati involontariamente o senza autorizzazione, ad esempio a causa di errori di funzionamento, malfunzionamenti, interruzioni di corrente, contaminazione o malware.

Tuttavia, la perdita di dati può anche derivare da danni, perdita o furto di dispositivi o supporti di dati. Questo rischio è spesso particolarmente elevato per i dispositivi mobili e i supporti dati mobili.

Inoltre, va notato che molti sistemi IT mobili non sono sempre online. I dati memorizzati su questi sistemi non sono quindi sempre aggiornati. Quando gli inventari dei dati sono sincronizzati tra i sistemi IT mobili e i sistemi IT fissi, i dati possono andare persi a causa di disattenzioni o malfunzionamenti.

Esempi:

- Lo smartphone cade dal taschino della camicia e si frantuma sulle piastrelle, un tablet viene recuperato dal cane invece del giornale, purtroppo con conseguenze. Questi e altri eventi simili sono la causa di molte perdite totali di dati su dispositivi finali mobili.
- Esistono programmi malware che eliminano specificamente i dati sui sistemi informatici infetti. Con alcuni malware, la funzione di cancellazione non viene eseguita immediatamente dopo l'infezione, ma solo quando si verifica un evento predefinito, ad esempio quando l'orologio del sistema raggiunge una certa data.
- Molti servizi Internet possono essere utilizzati per memorizzare informazioni online. Se la password viene dimenticata e non viene memorizzata, può accadere che le informazioni memorizzate non siano più accessibili se non viene offerta una procedura adeguata per la reimpostazione della password tramite il servizio Internet.
- I dischi rigidi e gli altri supporti di memoria di massa hanno una durata limitata. Se non vengono adottate misure di ridondanza adeguate, i dati possono andare persi a causa di difetti tecnici.

G 0.46 Perdita di integrità di informazioni riservate

L'integrità delle informazioni può essere compromessa da varie cause, come manipolazioni, comportamenti scorretti di persone, funzionamento errato di applicazioni, malfunzionamento di software o errori di trasmissione.

- Le informazioni possono andare perse a causa dell'invecchiamento dei supporti di dati.
- Errori di trasmissione: durante la trasmissione dei dati possono verificarsi errori di trasmissione.
- Malware: Il malware può alterare o distruggere interi set di dati.
- Inserimenti errati: inserimenti errati possono portare a transazioni indesiderate che spesso passano inosservate per molto tempo.
- Gli aggressori possono cercare di manipolare i dati per i propri scopi, ad esempio per ottenere l'accesso ad altri sistemi informatici o a stock di dati.
- Manipolando il database degli indici, gli archivi elettronici possono essere indotti ad archiviare o riprodurre documenti falsificati.

Se le informazioni non sono più integre, possono sorgere diversi problemi:

- Nel caso più semplice, le informazioni non possono più essere lette, cioè elaborate.
- I dati possono essere inavvertitamente o deliberatamente falsificati in modo da trasmettere informazioni false. In questo modo, ad esempio, si possono effettuare bonifici di importo sbagliato o al destinatario sbagliato, si possono manipolare i dati del mittente delle e-mail o molto altro ancora.
- Se i set di dati criptati o compressi perdono la loro integrità (basta la modifica di un bit), potrebbero non essere più in grado di essere decifrati o decompressi.
- Lo stesso vale per le chiavi crittografiche; anche in questo caso è sufficiente la modifica di un bit perché le chiavi diventino inutilizzabili. Questo porta anche al fatto che i dati non possono più essere decifrati o controllati per verificarne l'autenticità.
- I documenti conservati negli archivi elettronici perdono valore probatorio se non è possibile dimostrarne l'integrità.

G 0.47 Effetti collaterali dannosi di attacchi informatici

Gli attacchi sostenuti dall'IT possono avere effetti che:

- non sono previsti dagli attaccanti;
- colpiscono gli oggetti non direttamente attaccati;
- danneggiano terze parti non coinvolte.

Ciò è dovuto all'elevata complessità e al collegamento in rete delle moderne tecnologie informatiche, nonché al fatto che le dipendenze degli oggetti bersaglio attaccati e dei processi associati non sono solitamente evidenti.

Ciò può portare, tra l'altro, a valutare in modo errato l'effettiva necessità di protezione degli oggetti bersaglio o a far sì che i responsabili degli oggetti bersaglio non abbiano alcun interesse personale a porre rimedio alle carenze di tali oggetti.

Esempi:

- I bot installati sui sistemi IT, che gli aggressori possono utilizzare per effettuare attacchi DDoS (Distributed Denial-of-Service), spesso non rappresentano una minaccia diretta per i sistemi IT infettati, poiché gli attacchi DDoS sono solitamente diretti contro sistemi IT di terzi.
- Le vulnerabilità dei dispositivi IoT nelle WLAN possono essere utilizzate dagli autori come gateway per attaccare altri dispositivi più importanti nella stessa WLAN. Pertanto, tali dispositivi IoT devono essere protetti, anche se di per sé hanno solo un basso livello di necessità di protezione.
- Gli attacchi ransomware ai sistemi IT possono innescare reazioni a catena in determinate circostanze e quindi colpire anche le infrastrutture critiche. Questo potrebbe a sua volta portare a colli di bottiglia per l'approvigionamento della popolazione, anche se gli aggressori potrebbero non averne l'intenzione.