LA GESTIONE DELLA SICUREZZA E IL RISCHIO INFORMATICO

Il tema della sicurezza informatica è diventato molto importante per la pubblica amministrazione, perché va di pari passo con l'estensione e lo sviluppo della digitalizzazione dei servizi pubblici, quindi più questi diventano digitali e più si deve garantire che questa digitalizzazione sia adeguata.

SICUREZZA INFORMATICA

- Le difese messe a punto dalla sicurezza informatica devono essere solide e stratificate. La protezione dei sistemi informativi è un percorso che richiede l'adozione di diverse misure, da soluzioni tecnologiche alla formazione degli utenti fino all'impostazione e all'implementazione di politiche efficaci.
- Una buona implementazione delle misure minime di sicurezza informatica in tutta l'organizzazione, politiche di sicurezza adeguate e processi di segnalazione di incidenti facili da eseguire, contribuiranno a mitigare il rischio di attacchi e costituiscono la base per una sicurezza prolungata nel tempo.
- È fondamentale che i membri della PA comprendano e seguano le politiche di sicurezza della propria organizzazione in modo tale che il personale sia in grado di identificare e segnalare una situazione di rischio.
- L'approccio migliore per proteggere un sistema informativo, è garantire che ogni sua componente abbia un proprio meccanismo di protezione .

4 FASI DI ATTACCHI INFORMATICI E QUALI SONO LE AZIONI CHE SIPOSSONO METTERE IN CAMPO PER MITIGARE GLI ATTACCHI INFORMATICI?

IDENDIFICAZIONE DEL TARGET

Si identifica l'obiettivo da colpire e se ne studiano le mosse. Attraverso tecniche come il "social engineering" si raccolgono informazioni sul target e sul sistema di sicurezza.

INTRUSIONE

Grazie alle informazioni raccolte si cerca di ottenere il controllo del dispositivo da remoto. Attraverso il "phishing" è possibile appropriarsi delle credenziali del network di protezione o tentare di installare un malware.

STUDIO DEL NETWORK

Nel corso di tentativi di mappare rete, porte di accesso e vulnerabilità, si individuano data base ed eventuali access point.

ACCESSO AI DATI

Con le credenziali di accesso ottenute, si prende il controllo dei sistemi informatici e dei relativi dati. Per mantenere l'accesso ,si cercherà di installare strumenti come "backdoors", "rootkits " o "trojan".

AGID

AgID supporta le amministrazioni nelle attività di progettazione e pianificazione di strategie utili ad assicurare la resilienza dell'infrastruttura informatica nazionale della PA.
Anche a fronte di un considerevole aumento di incidenti informatici o azioni ostili volti a compromettere il corretto funzionamento dei sistemi informativi o dei servizi erogati, le iniziative di AgID (Direttiva del Presidente del Consiglio dei Ministri, 1 agosto 2015) sono volte ad agevolare un sistema di prevenzione e di risposta efficiente delle singole amministrazioni.

COME PUO ESSERE GESTITO IL RISCHIO NELLE PA?

- La Pubblica Amministrazione, nel perseguire le proprie finalità istituzionali, si avvale di uffici e professionalità e tecnologie volti ad assicurare informazioni e servizi alla collettività.
- La sicurezza riveste un'importanza fondamentale per assicurare la disponibilità, l'integrità, la riservatezza delle informazioni, dei servizi offerti e della resilienza della complessa macchina amministrativa.
- A seconda della complessità del sistema informativo e della realtà organizzativa dell'amministrazione, le attività di gestione del rischio possono tradursi in controlli di natura tecnologica, organizzativa e procedurale utili a valutare il livello di sicurezza informatica e volti a contrastare le minacce informatiche più frequenti, all'interno di un percorso continuo di monitoraggio e miglioramento.

LA GESTIONE DEL RISCHIO

Proteggere le nostre informazioni vuol dire analizzare le situazioni e gli ambiti in cui sono trattate e valutare i rischi di sicurezza associati.

Il risk management si compone dei diversi processi di risk identification, attraverso cui si identificano i rischi, risk evaluation e risk assessment per la loro valutazione e infine il loro trattamento, il risk treatment.

In molti Paesi, i legislatori prevedono norme che disciplinano iniziative volte:

- alla riduzione o alla gestione del rischio connesso alle attività di sistemi complessi,
- a contenere o evitare eventuali effetti negativi che una minaccia (evento malevolo o incidente) comporterebbe sulle persone, sulle cose e sull'ambiente.

LAVORO DI A. V. E V. R.

LA SICUREZZA INFORMATICA NELLE PUBBLICHE AMMINISTRAZIONI

La gestione della sicurezza e del rischio informatico nelle p.a.

A. M. G.

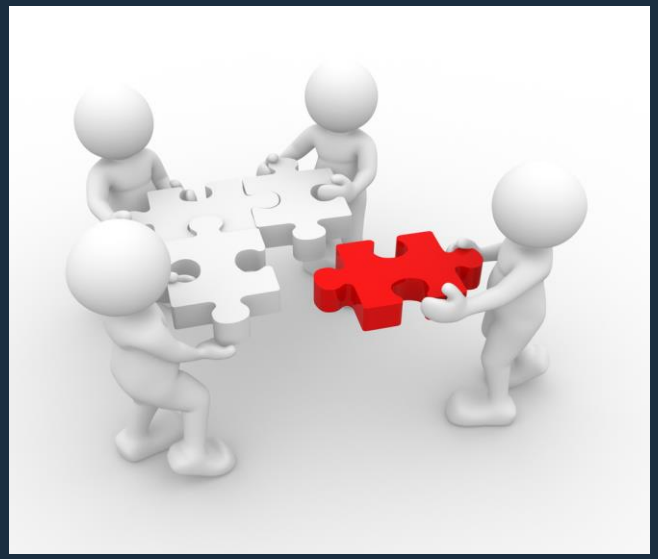
Agid e PA

La Pubblica Amministrazione, nel perseguire le proprie finalità istituzionali, si avvale di uffici e professionalità e tecnologie volti ad assicurare informazioni e servizi alla collettività.

La sicurezza riveste un’importanza fondamentale per assicurare la disponibilità, l’integrità, la riservatezza delle informazioni, dei servizi offerti e della resilienza della complessa macchina amministrativa.

La cybersecurity non deve essere percepita come una moda, infatti basta consultare il Global Risk Report del World Economic Forum per rendersene conto. La superficie di attacco è sempre di più in aumento, perché aumenta il numero degli utenti e con essi gli indirizzi IP, il traffico di rete e il volume di dati che questo trasporta.

E’ indispensabile approfondire la conoscenza sugli attacchi informatici che potrebbero colpire anche i servizi pubblici e sulle azioni da mettere in campo per mitigare tali attacchi. L’obiettivo è quello di assicurare la continuità dei servizi pubblici, gestendo le attività di pianificazione, coordinamento e monitoraggio della sicurezza informatica, specialmente da parte del Responsabile per la Transizione al Digitale. Vale per tutte le amministrazioni che erogano servizi ai cittadini ed alle imprese.



A seconda della complessità del sistema informativo e della realtà organizzativa dell'amministrazione, le attività di gestione del rischio possono tradursi in controlli di natura tecnologica, organizzativa e procedurale utili a valutare il livello di sicurezza informatica e volti a contrastare le minacce informatiche più frequenti, all'interno di un percorso continuo di monitoraggio e miglioramento.

Servizi sicuri

La gestione del rischio informatico è una parte importante della progettazione e della gestione continuativa del sistema informativo, nell'ottica dei principi di security by design. Non può essere considerata come un'azione una tantum o ex post dei controlli di sicurezza. Già nella fase di definizione dei requisiti, la progettazione di un servizio deve prevedere una valutazione del rischio che permetta di appurare la necessità di proteggere il servizio stesso e quanto una soluzione tecnica faciliti o, al contrario, ostacoli l'adozione di controlli adeguati.

IL RUOLO DI AGID

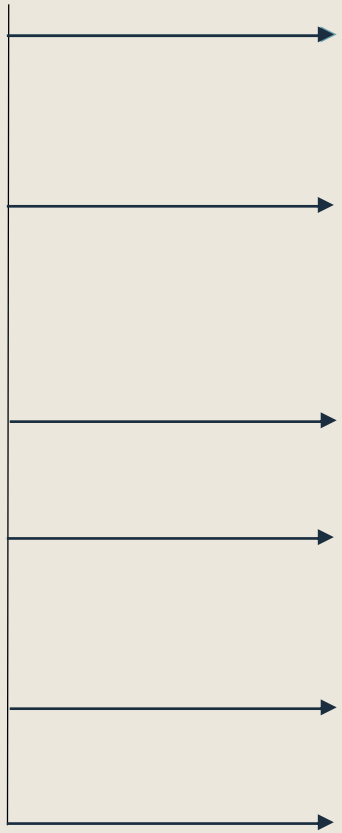
- AgID supporta le amministrazioni nelle attività di progettazione e pianificazione di strategie utili ad assicurare la resilienza dell'infrastruttura informatica nazionale della PA. Anche a fronte di un considerevole aumento di incidenti informatici o azioni ostili volti a compromettere il corretto funzionamento dei sistemi informativi o dei servizi erogati, le iniziative di AgID (Direttiva del Presidente del Consiglio dei Ministri, 1 agosto 2015) sono volte ad agevolare un sistema di prevenzione e di risposta efficiente delle singole amministrazioni.

- AgID ha sviluppato una metodologia di gestione del rischio, a partire da un benchmark internazionale di buone prassi pubbliche e private, per:

Poter essere supportata da uno strumento applicativo fruibile da tutte le PA e integrato con altre infrastrutture IT centrali.

Poter essere applicata a tutti gli enti della Pubblica Amministrazione italiana, diversi per dimensioni, complessità tecnologiche e di erogazione dei servizi verso imprese, cittadini e nei confronti di altre entità pubbliche;

Il progetto ha l’obiettivo di:



- definire un processo di analisi del rischio per poter ottenere, nel medio termine, una stima del livello di rischio cyber cui è esposta ciascuna PA;
- rendere autonoma ogni PA nella pianificazione di interventi per il trattamento del rischio al fine di ridurlo ad un livello ritenuto accettabile (risk appetite);
- ricondurre tali interventi a convenzioni già attive nell’ambito dei contratti quadro;
- consentire il monitoraggio dell’implementazione di tali interventi alle PA che hanno affrontato l’analisi del rischio;
- creare uno strumento di monitoraggio AgID esteso su tutti gli enti della PA;
- diffondere tra tutti gli stakeholders coinvolti la cultura della gestione del rischio cyber.

In particolare, la diffusione della cultura del rischio cyber fa riferimento a:

- lo sviluppo sicuro dei servizi, sulla base della rispondenza alle linee guida sullo sviluppo sicuro del software ed all'utilizzo del tool di risk assessment di AgID;
- la familiarità con i principi dell'analisi dinamica (DAST) e statica (SAST) del software;
- l' introduzione all'approccio del privacy/security by design.

“In un mondo digitale dove tutti i dati sono disponibili online è evidente che lo Stato debba rafforzare la propria capacità di difenderSI e difenderCI da attacchi cibernetici.

La transizione digitale richiede uno sforzo significativo di ammodernamento della cybersecurity nazionale, che protegga sia le persone sia le infrastrutture. Sarà anche sempre più importante assicurare a imprese, PA e cittadini che hardware, software, applicazioni, e algoritmi siano e si mantengano sicuri e ispezionabili.

Non da ultimo, il comparto cybersecurity ha una fondamentale importanza sul piano geostrategico, che deve collocare l’Italia chiaramente nel quadro Europeo e Atlantico. Dovremo considerare sempre più tra i beni nazionali da proteggere anche il diritto alla Privacy. La trasformazione digitale implica che gran parte delle informazioni sull’identità di una persona, molte delle quali sensibili, verranno custodite in rete. È necessario garantire, in tutto e per tutto, che questi dati siano inviolabili.”


identity
digital
information
system
Internet
public
identities
user
example
subject
metasystem
contexts
need
should
systems
claim
party
control
different
being
services
parties
claims
through
channel
identifying
between
government
way
context
any
laws
users
world
human
layer
want
Identity
sites
allow
doubt
privacy
make
law
work
key
know
time
things
individuals
experience
applications
universal
unique
risk
site
consumer
identifier
service
omni-directional
multiple
certain
certificates
individual
therefore
made
another
Laws
word
relying
failures
ad
patchwork
connecting
across
one-offs
Analytics
specific
essential
Passport
set
relationship
into
solution
computing
technology
user's
involved
kinds
industry
identifiers
dealing
computer
definition
before
required
number
Starts
allows
devices
define
unifying
cyber
thing
aware
consent
built
least
prevent
wants
device
justifiable
described
mean
rather
place
identify
issued
technologies
needs
ceremony
relationships
result
represents
disclosing
issues
trust
successes
framework
business
web
private
sense
important
communication
existence
policy
single
hoc
understand
Microsoft
further
something
situation
currently
beacon
distributed
discussion
protect
projector

M. M.

INDICE:

- PRIVACY;
- IDENTITA' DIGITALE;
- SPID;
- CODICE AMMINISTRAZIONE DIGITALE.

PRIVACY

Il termine **privacy** indica il **diritto alla riservatezza** delle informazioni personali e della propria vita privata.

Oggi si intende anche il diritto a esprimere liberamente le proprie aspirazioni, quindi l'autodeterminazione e la sovranità su se stessi, il riconoscersi parte attiva nel rapporto con le istituzioni e nel rispetto reciproco delle libertà.

IDENTITA' DIGITALE

Si tratta dell'insieme d'informazioni che, all'interno di un determinato sistema informatico, si riferiscono a una specifica persona. Quanto più elevato è il livello di complessità all'interno del sistema informatico, tanto più approfondite saranno le informazioni relative alla persona.

Con l’identità digitale, è possibile stabilire che una data persona in un preciso momento ha avuto accesso a un sistema informatico e sta compiendo delle determinate azioni. L’accesso al sistema informatico avviene tramite delle credenziali che identificano univocamente la persona e di cui soltanto il soggetto dovrebbe essere in possesso.

IDENTITA' DIGITALE: SPID

Può avere diverse implicazioni che permettono di semplificare o rendere più sicuri determinati processi:

- **SPID** sta per Sistema pubblico d'identità digitale. Una volta iscritti sul sito *gov.it*, si riceve la propria SPID personale con la quale è possibile, utilizzando gli strumenti digitali, gestire tutte le comunicazioni da e verso la pubblica amministrazione.

CODICE AMMINISTRAZIONE DIGITALE

Il Codice dell'amministrazione digitale rappresenta il punto di riferimento normativo per guidare la trasformazione digitale della PA in Italia fornendo utili indicazioni anche a cittadini e provider, per la corretta gestione di documenti informatici e processi amministrativi digitalizzati.