ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Prediccions i tendències clau Ciberseguretat pel 2023

Informe elaborat per l'**Agència Nacional de Ciberseguretat d'Andorra**

ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

- En els últims anys, hem vist com **la ciberseguretat es trasllada del departament de TI als Comitès de Direcció de les organitzacions**. A mesura que han proliferat els atacs i han augmentat les possibles sancions, tant les normatives, com la pèrdua de confiança del client/usuari, s'ha convertit en una prioritat en tots els nivells de l'organització.
- Sovint pensem en la ciberseguretat com una batalla contínua entre pirates informàtics i delinqüents, i experts en seguretat, que augmenta constantment a causa dels continus avenços tecnològics. Aquest és el costat "glamurós" del negoci que de vegades veiem representat en programes de televisió i pel·lícules. De fet, les amenaces sovint provenen d'estats estrangers hostils o de cervells criminals astuts i experts en tecnologia. En realitat, però, és probable que sorgeixin **amenaces a causa de xarxes i/o sistemes mal protegits** que deixen dades confidencials exposades accidentalment, o **empleats desprevinguts o indiscrets** que fan servir dispositius no segurs mentre treballen des de casa.
- El canvi cap a una **cultura de teletreball** que es va iniciar durant la pandèmia de Covid-19, i que ha persistit en moltes organitzacions, així com **la propagació d'Internet de les coses** (IoT) en totes les àrees dels negocis i la societat, significa que mai hi ha hagut més oportunitats perquè **la manca de ciberseguretat provoqui problemes greus i elevades despeses en les organitzacions**.
- Per tot això, **la ciberseguretat ha de ser una prioritat en l'agenda de totes les organitzacions de cara al 2023**. En aquest sentit, s'elabora aquest document en que es presenten algunes de les **tendències clau del 2023 en matèria de ciberseguretat**.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

1

Prediccions i tendències clau
Ciberseguretat 2023

La ciberseguretat de la feina des de casa es converteix en una prioritat per a les empreses

www.anc.ad

ANDORRA DIGITAL

1

Prediccions i tendències clau

Ciberseguretat 2023

www.anc.ad

ANC-AD

La ciberseguretat de la feina des de casa es converteix en una prioritat per a les empreses

Recentment, una prioritat de seguretat cibernètica per a moltes organitzacions ha estat protegir els milions de dispositius a tot el món que s'utilitzen per a la llar i el treball remot des del començament de la pandèmia. Abans de la pandèmia, quan tots estàvem a l'oficina, era bastant simple per als agents de seguretat, probablement ubicats als departaments de TI, revisar i actualitzar regularment els ordinadors portàtils i els telèfons intel·ligents de l'empresa. Això va fer que fos relativament simple assegurar-se que estiguessin lliures de spywar i malware i que estiguessin executant les últimes versions de programari antivirus i altres mesures preventives. A l'any 2023, quan és més probable que mai que els treballadors facin servir dispositius personals per connectar-se de forma remota a les xarxes de treball, ha sorgit un nou conjunt de desafiaments.

Connectar-se a xarxes amb dispositius no segurs pot portar que els empleats siguin víctimes inadvertides d'atacs de phishing, en els quals els atacants enganyen els usuaris perquè divulguin les seves contrasenyes. Amb més persones treballant de forma remota, és cada vegada més probable que ens trobem treballant en equips en els quals no ens coneixem bé i correm el risc de caure en estafes de suplantació d'identitat. També permet atacs de ransomware, on s'injecta programari en xarxes que esborren dades valuoses llevat que els usuaris paguin un rescat als atacants. El risc d'això també augmenta en situacions de treball remot, on és més probable que els dispositius quedin desatesos.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

2

Prediccions i tendències clau
Ciberseguretat 2023

Construint una cultura conscient de la seguretat

www.anc.ad

ANDORRA DIGITAL

2

Prediccions i tendències clau

Ciberseguretat 2023

www.anc.ad

ANC-AD

Construint una cultura conscient de la seguretat

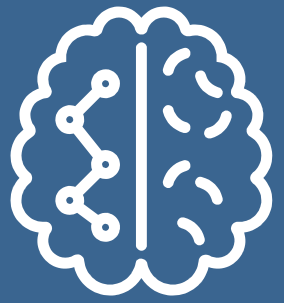
Potser el pas més important que es pot donar en qualsevol organització és assegurar-se que està treballant per iniciar i fomentar una cultura de consciència sobre els problemes de ciberseguretat. Avui dia, ja no és suficient que els ocupadors o els empleats simplement pensin en la seguretat cibernètica com un problema del qual s'ha d'ocupar el departament de TI. De fet, desenvolupar una consciència de les amenaces i prendre precaucions bàsiques per garantir la seguretat hauria de ser una part fonamental de la descripció del treball de tots al 2023.

Els atacs de phishing es basen en mètodes d'"enginyeria social" per enganyar als usuaris perquè divulguin informació valuosa o instal·lin malware en els seus dispositius. No es necessiten coneixements tècnics per aprendre a ser conscient d'aquest tipus d'atacs i prendre les precaucions bàsiques per no ser víctima. De la mateixa manera, les habilitats bàsiques de seguretat, com l'ús segur de contrasenyes i el desenvolupament d'una comprensió de l'autenticació de multi factors, s'han d' ensenyar de manera generalitzada i actualitzar-se contínuament. Prendre precaucions bàsiques com aquesta per fomentar una cultura de conscienciació sobre la seguretat cibernètica ha de ser un element central de l'estratègia comercial en les organitzacions que volen assegurar-se de desenvolupar resiliència i preparació en els propers 12 mesos.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

3



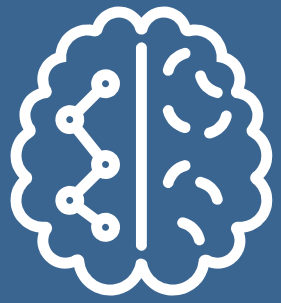
Prediccions i tendències clau
Ciberseguretat 2023

La intel·ligència artificial (IA) juga un paper cada vegada més destacat en la ciberseguretat

www.anc.ad

ANDORRA DIGITAL

3



Prediccions i tendències clau

Ciberseguretat 2023

www.anc.ad

ANC-AD

La intel·ligència artificial (IA) juga un paper cada vegada més destacat en la ciberseguretat

A mesura que la quantitat d'intents d'atacs cibernètics ha crescut ràpidament, s'ha tornat cada vegada més complicat per als experts en ciberseguretat humana reaccionar davant de tots ells i predir on s'esdevindran els atacs més perillosos a continuació. Aquí és on entra en joc la IA. Els algoritmes d' aprenentatge automàtic poden examinar la gran quantitat de dades que es mouen a través de les xarxes en temps real de manera molt més efectiva que els humans i aprendre a reconèixer patrons que indiquen una amenaça.

Desafortunadament, gràcies a la disponibilitat cada vegada més gran d'IA, els pirates informàtics i els delinqüents també són cada vegada més competents en el seu ús. Els algoritmes d'IA s'utilitzen per identificar sistemes amb seguretat feble o que probablement continguin dades valuoses entre els milions de computadores i xarxes connectades a Internet. També es pot utilitzar per crear una gran quantitat de correus electrònics de phishing personalitzats dissenyats per enganyar els receptors perquè divulguin informació confidencial i siguin cada vegada més bons per evadir els sistemes de defensa de correu electrònic automatitzats dissenyats per filtrar aquest tipus de correu.

Aquesta és la raó per la qual s'utilitza la IA en la ciberseguretat, ja que els pirates informàtics i els agents de seguretat competeixen per garantir que els algoritmes més nous i sofisticats funcionin del seu costat i no per a l'oposició.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

4

Prediccions i tendències clau
Ciberseguretat 2023

Internet de les coses amb xarxa 5G i seguretat al núvol

www.anc.ad

ANDORRA DIGITAL

4

Prediccions i tendències clau

Ciberseguretat 2023

www.anc.ad

ANC-AD

Internet de les coses amb xarxa 5G i seguretat al núvol

L'arquitectura 5G és comparativament nova en la indústria i requereix molta investigació per trobar llacunes que facin que el sistema sigui segur contra atacs externs. Cada pas de la xarxa 5G pot portar una gran quantitat d'atacs a la xarxa que tal vegada no siguem conscients.

Com més dispositius connectem i connectem en xarxa, més portes i finestres potencials existeixen que els atacants poden fer servir per ingressar i accedir a les nostres dades. I al 2023, prediuen els analistes de Gartner, hi haurà 43 mil milions de dispositius connectats a IoT al món.

Els dispositius IoT, que van des de dispositius portàtils intel·ligents fins a electrodomèstics, automòbils, sistemes d'alarma d'edificis i maquinària industrial, sovint han demostrat ser un malson per als qui tenen responsabilitat en la ciberseguretat. Això es deu al fet que, atès que sovint no s'utilitzen per emmagatzemar dades confidencials directament, els fabricants no sempre s'han centrat a mantenir-les segures amb actualitzacions i pegats de seguretat freqüents. Això ha canviat recentment, ja que s'ha demostrat que fins i tot quan no emmagatzemen dades per si mateixes, els atacants sovint poden trobar formes d'usar-les com portes d'enllaç per accedir a altres dispositius en xarxa que podrien fer-ho. Avui, per exemple, és menys probable que trobi un dispositiu enviat amb una contrasenya o PIN predeterminats que no requereixin que l'usuari configuri els seus propis, com ocorria amb freqüència en el passat.

Al 2023, haurien d'entrar en vigor una sèrie d'iniciatives governamentals a tot el món dissenyades per augmentar la seguretat al voltant dels dispositius connectats, així com els sistemes al núvol i les xarxes que els vinculen a tots.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

5

Prediccions i tendències clau
Ciberseguretat 2023

Guerra cibernètica: atacants internacionals patrocinats per estats apunten tant a empreses, com a governs

ANDORRA DIGITAL

5

Prediccions i tendències clau

Ciberseguretat 2023

www.anc.ad

ANC-AD

Guerra cibernètica: Atacants internacionals patrocinats per estats apunten tant a empreses, com a governs

Els estats-nació amb freqüència participen en l'espionatge cibernètic i el sabotatge en un intent de soscavar governs hostils o competidors o per accedir a secrets. En l'actualitat, però, és cada vegada més probable que les empreses i les organitzacions no governamentals (ONG) es trobin en el punt de mira dels actors estatals.

Des de l'atac de ransomware WannaCry del 2017 , que es creu que va ser perpetrat per pirates informàtics afiliats al govern de Corea del Nord, hi ha hagut centenars de milers d'atacs a servidors de tot el món que les agències de seguretat creuen que poden rastrejar-se fins a governs estrangers.

Al 2023, més de 70 països han de celebrar eleccions governamentals, esdeveniments que amb freqüència són blanc d'atacs per part d'interessos estrangers hostils. A més de la pirateria i els atacs cibernètics a la infraestructura, això prendrà la forma de campanyes de desinformació a les xarxes socials. Això sovint implica tractar d'influir en els resultats a favor dels partits polítics les victòries dels quals beneficiarien el govern de l'estat hostil. I la guerra cibernètica, sens dubte, seguirà sent un element clau en el conflicte armat, amb un analista que va dir sobre la guerra entre Rússia i Ucraïna que "el digital és una part important d'aquesta guerra, igual que la lluita sobre el terreny".

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

6

Prediccions i tendències clau
Ciberseguretat 2023

Atacs de ransomware més sofisticats

www.anc.ad

ANDORRA DIGITAL

6

Prediccions i tendències clau

Ciberseguretat 2023

www.anc.ad

ANC-AD

Atacs de ransomware més sofisticats.

El panorama d'amenaces s'està expandint ràpidament, i els mals actors seran implacables en els seus esforços per dur a terme atacs més sofisticats l'any vinent.

El ransomware continuarà en els titulars, a mesura que els atacs es tornin més destructius i els actors d'amenaces desenvolupin noves tàctiques, tècniques i procediments (TTP) per mirar de mantenir-se un pas per davant dels proveïdors, mentre busquen aprofitar el poder cibernètic massiu de la computació quàntica sempre que sigui possible. Si bé aquesta tecnologia defineix una nova era en l'evolució d'avenços en dades, la computació quàntica també ofereix un nou conjunt d'oportunitats perquè els actors d'amenaces obtinguin accés a informació confidencial que podria immobilitzar les organitzacions.

Els equips de seguretat han d'estar atents i ser proactius, ja que els atacants continuen buscant formes innovadores i creatives d'evitar les solucions de ciberseguretat.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

7

Prediccions i tendències clau
Ciberseguretat 2023

Les infraestructures crítiques i el sector públic continuaran sent objectius atractius

www.anc.ad

ANDORRA DIGITAL

7

Prediccions i tendències clau

Ciberseguretat 2023

www.anc.ad

ANC-AD

La infraestructura crítica i el sector públic continuaran sent objectius atractius.

A mesura que els atacs cibernètics es tornen més sofisticats, la creació de comunitats col·laboratives entre els sectors públic i privat serà crucial per sincronitzar les operacions i prendre mesures preventives com un front unificat per a les amenaces a la infraestructura crítica.

El sector públic s'ha convertit en un objectiu privilegiat per als ciberdelinqüents. Armats amb botnets automatitzats, els pirates informàtics furguen en els sistemes informàtics per localitzar "objectius". En els últims anys, les agències governamentals estatals i locals de gran part del món han estat víctimes d'atacs cibernètics.

La seguretat heretada està demostrant ser ineficaç contra la creixent legió de ciberamenaces diverses, sofisticades i conflictives. Les agències públiques recopilen i emmagatzemen dades confidencials. Igual que el sector privat, les institucions governamentals s'han tornat digitals. L'addició del núvol, els dispositius mòbils i SaaS ha ampliat la superfície d'atac d'una organització i aclareix encara més que la seva seguretat cibernètica és tan forta com el seu punt més feble.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

8

Prediccions i tendències clau
Ciberseguretat 2023

SaaS i el núvol

www.anc.ad

ANDORRA DIGITAL

8

Prediccions i tendències clau

Ciberseguretat 2023

www.anc.ad

ANC-AD

SaaS i el núvol

A mesura que les empreses lluiten per adaptar-se ràpidament a les regulacions canviants i complexes en el panorama de la seguretat cibernètica, moltes estan adoptant una estratègia més flexible i àgil per tenir èxit. Les aplicacions basades en el núvol per a la seguretat i els serveis SaaS estan cada vegada més esteses, ja que són més capaces d'escalar amb les necessitats de les companyies que cada vegada són més canviants.

Les solucions al núvol ofereixen a les empreses més llibertat per accedir i distribuir tecnologies de seguretat per a tots els seus usuaris, els quals cada vegada estan més dispersos geogràficament. Això ha fet que l'entorn del núvol sigui una opció particularment popular entre les empreses flexibles amb treballadors distribuïts i híbrids on cal garantir la seva ciberseguretat.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

9

Prediccions i tendències clau
Ciberseguretat 2023

Majors amenaces pel sector sanitari

www.anc.ad

ANDORRA DIGITAL

9

Prediccions i tendències clau

Ciberseguretat 2023

www.anc.ad

ANC-AD

Majors amenaces pel sector sanitari

Si bé totes les indústries poden ser fàcilment atacades pels ciberdelinqüents en el panorama digital actual, alguns sectors han estat experimentant més desafiaments que la majoria. El sector de la salut en particular ha estat un objectiu principal de moltes amenaces importants en els darrers anys. Per tant, s'espera que el sector de la ciberseguretat per a la indústria assoleixi un valor al voltant de 33.600 milions de dòlars per al 2027.

Tal vegada la major amenaça a la qual s'enfronta el sector sanitari és el risc d'una violació de dades. A l'any 2021, al voltant d'11.7 mil milions de registres van ser robats o exposats per ciberdelinqüents. Això ha portat a posar un major èmfasi en les seves xarxes i entorns de seguretat digitals del sector salut on a més s'uneix que cada vegada hi ha més dispositius IOT de salut (quiròfan connectat , etc...) fent créixer el terreny de joc exposat als perills del ciberespai.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

10

Prediccions i tendències clau
Ciberseguretat 2023

Junta directiva amb més coneixement cibernètic i inversió

www.anc.ad

10 Junta directiva amb més coneixement cibernètic i inversió.

L'èxit empresarial i la ciberseguretat van de la mà. A mesura que evoluciona el paper de la junta directiva en la supervisió del risc cibernètic, no es pot subestimar la importància d'un diàleg sòlid amb els experts cibernètics dins d'una organització. Sense una comunicació propera entre les juntes directives i l'equip cibernètic de risc, l'organització podria córrer un risc encara més gran. Si això sona com un exercici de preparació de ciberseguretat, és perquè ho és.

Preparar professionals de ciberseguretat amb perspicàcia comercial perquè la junta actuï com la veu de la raó educada no és una mala idea.
Les millors empreses prosperen perquè tenen persones al cim que poden exercir el control sobre la base d'una presa de decisions informada quan s'acosta una crisi. Deixar la ciberseguretat fora d'aquesta equació d'èxit al 2023 és un joc arriscat. Els equips de ciberseguretat han d' equipar la junta amb el següent com a punt de partida:

- Una anàlisi clara dels riscos cibernètics actuals que enfronten tots els aspectes del negoci (no només TI).
- Un resum dels incidents cibernètics recents, com es van manejar i les lliçons apreses.
- Fulls de ruta a curt i llarg termini que descriuen com l'empresa continuarà desenvolupant les seves capacitats cibernètiques per abordar amenaces noves i ampliades, incloses les responsabilitats relacionades establertes per garantir el progrés.
- Mètriques significatives que brinden indicadors de risc i rendiment essencials de recolzament de la gestió exitosa dels riscos cibernètics de màxima prioritat que s'estan gestionant

ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Prediccions i tendències clau Ciberseguretat 2023

Informe elaborat per **ANC-AD**