5G FORBINDELSE (MOBILNETVÆRK)

5G er den femte generation eller udgave af standarden for, hvordan mobilnetværket fungerer.

Hvordan fungerer det

Lige som forgængeren, 4G, fungerer systemet ved, at de forbundne enheder er forbundet via radio til en lokal antenne og på denne måde får adgang til telefoni og internet.

Fordelen ved den nye generation er, at man får højere båndbredde og dermed mulighed for højere hastighed. 5G lover således hastigheder op mod 10 gigabit i sekundet. Det er en hastighed, der for alvor kan konkurrere med kabler, ligesom det giver nye muligheder for Internet of Things (IoT) og forbundne systemer, der udveksler data. For at bruge 5G skal man have en mobiltelefon, der understøtter teknologien.

Angreb og forsvar

5G er ikke en trussel i forhold til cybersikkerhed og kræver som sådan ikke særligt forsvar, men giver alene mulighed for endnu mere fart på det mobile internet. Højere hastigheder betyder selvfølgelig flere services, der bruger data. Der vil for eksempel komme nye muligheder for dataudveksling inden for det, man kalder Internet of Things. Når der kommer flere services, bliver det også mere interessant for angribere. Det betyder, at det i endnu højere grad er nødvendigt, at udviklerne af denne type systemer sørger for, at sikkerheden er i orden.

Historie

De første muligheder for internet over mobilnetværket kom med 2G helt tilbage i 1991. Det mobile bredbånd i Danmark tog først for alvor

fart med udbredelsen af smartphones (smarte telefoner), herunder Apples anden generation af deres iPhone, der understøttede 3G, og med introduktionen af Android-styresystemet i 2008.

Spillet

Kortet er et aktionskort, der kan spilles under din tur og koster fem porte at spille. Træk fem kort fra bunken. Hvis det betyder, du nu har mere end fem kort på hånden, skal du kassere de overskydende kort, så du højest har fem kort på hånden. De kasserede kort og dette kort smides i kortbunken. Kortet giver således mulighed for at udskifte mange kort på hånden eller hurtigt få fyldt op, hvis man har spillet det meste af sin hånd.

BACKUP

En sikkerhedskopi - eller en backup - er en kopi af data som, hvis de originale data går tabt eller bliver ødelagt, kan bruges til at genskabe disse.

Hvordan fungerer det

En backup eller en sikkerhedskopi er en kopi af de filer, man ønsker at beskytte. I simpleste form laver man simpelthen manuelt en kopi og gemmer denne på et andet lagringsmedier. Det kan være på et usb-medie, et netværksdrev eller en online tjeneste.

Mere avancerede backupsystemer gemmer løbende ændringer i enten bestemte mapper eller foldere på computeren eller af hele computersystemet.

Angreb og forsvar

Backup beskytter ikke bare mod angreb men også mod fejl og uheld. Man kan altså bruge sin backup, hvis computeren går i stykker, eller hvis man sletter eller redigerer dokumenter ved en fejl, så de ikke kan genskabes. I forhold til angreb på computersystemer kan en sikkerhedskopi genskabe hele systemet, men det kommer altid med en pris: Dels kan det være tidskrævende at genskabe systemet ved hjælp af en backup, dels vil man miste de data, der er blevet ændret, siden backuppen blev lavet. Mange vira vil udnytte dette til at gemme sig i længere tid, inden de giver sig til kende, hvilket betyder, at også backuppen kan være inficeret.

Historie

Sikkerhedskopier kendes helt tilbage til 1950'erne, hvor man brugte hulkort. Ligesom gennemslagspapir kunne man også lave flere kopier af hulkortene for at sikre sig mod ødelagte eller beskadigede kort.

Senere kom harddisken til, men denne var meget dyr, og det var derfor almindeligt fra 1960'erne og helt op til i dag at anvende magnetbånd til backup. Disse er meget langsomme at skrive og læse data fra, men til gengæld billige at bruge. I forbindelse med hjemmecomputernes udbredelse blev det almindeligt at tage backup ved at kopiere filer til eksterne lagringsmedier som disketter og senere CD-rom, DVD og usb-medier, men også eksterne harddiske er, i takt med at priserne for disse er faldet, blevet brugt til backup. I dag er de fleste backupsystemer cloudbaserede og tilgås over internettet. Dette gør det hurtigere at skalere i takt med, at man får brug for mere plads. Samtidigt sikrer det, at backuppen fysisk befinder sig et andet sted end der, hvor den originale data skabes og bruges.

Spillet

Kortet er et reaktionskort og kan spilles, hvis du ikke har flere åbne porte. Du kan så spille dette kort og ofre yderligere tre kort fra hånden for at åbne 10 porte. Har du ikke tre kort, du kan ofre, kan du ikke spille dette kort. De ofrede kort og dette kort smides i kortbunken efter at være blevet spillet.

BIKBOK (SOCIALT MEDIE)

BikBok er et eksempel på en app, der indsamler data og sender det tilbage til appudvikleren. Dataindsamling kendes fra mange apps og tjenester. Ofte er dataindsamlingen nødvendig for at tjenesten fungerer. Data kan også anvendes til at forbedre tjenesten i kommende versioner. Der er i stigende grad kommet apps og tjenester, der indsamler en masse data alene for at kunne målrette reklamer, drive maskinlæring eller spionere på brugerne.

Hvordan fungerer det?

Det er især i forbindelse med apps på telefonen og besøg på hjemmesider, man taler om dataindsamling, men almindelige computerprogrammer kan også samle data om brugen og brugerne. Mobiltelefonernes styresystemer er i stigende grad blevet bedre til at kræve, at brugeren giver specifik tilladelse til, hvilke data de forskellige apps får adgang til, ligesom man i browserne kan få forskellige udvidelser, der advarer om hvilke data, der deles.

Angreb og forsvar

Mange tjenester kræver, at man deler sine data. Indenfor EU er man beskyttet af persondataforordningen, GDPR. Det kræves af tjenesteudbyderne, at de overholder en række regler og fortæller brugerne om, hvordan data anvendes. På mobiltelefoner skal man i dag give tilladelser til, hvilke data de enkelte apps har adgang til. Man bør være opmærksom på, om der er en passende sammenhæng mellem de data, appen beder om adgang til, og hvad appen skal kunne. En billedbehandlingsapp, der beder om adgang til telefonens billedmappe, er helt forståeligt, men beder samme app om adgang til dine kontakter eller telefonens GPS, kan det være, at man skal overveje at finde en anden app!

BIKBOK (SOCIALT MEDIE)

Historie

Dataindsamling har stort set altid fundet sted og siden industrialiseringen i stigende grad systematisk, men først med computere og ikke mindst automatisk dataopsamling er det blevet muligt at samle data i de store mængder, vi ser i dag. Med fremkomsten af sociale medier i den form, vi kender i dag, i slutningen af halvfemserne, er denne dataindsamling eksploderet.

Spillet

Kortet tvinger en anden spiller til at vise sin hånd og spille med åbne kort. Det koster 2 porte at spille, men giver ingen skade. Kortet er et aktionskort og kan derfor kun spilles, når det er din tur. Kortet kan spilles både som angreb og forsvar (altså både til spilleren til højre eller spilleren til venstre). Når man spiller kortet, placeres det foran den spiller, der nu skal spille med åbne kort, indtil denne spiller har afsluttet sin næste tur.

BOBBY (COMPUTERVIRUS)

Bobby er et eksempel på en computervirus. En computervirus er et computerprogram, som hele tiden forsøger at lave kopier af sig selv både til andre computere og til andre steder på den allerede inficerede computer. Udover at computervira bruger af computerens ressourcer som processer, harddisk og hukommelse, så er forskellige computervira også lavet mere eller mindre destruktive lige fra at give relativt harmløse beskeder til brugeren til at forsøge at ødelægge, slette eller kryptere computerens styresystem, programmer og dokumenter. Med udbredelsen er internettet er vira blevet mere destruktive og farlige, da de oftest bruges til at overtage computeren (for eksempel til at lave andre angreb), stjæle kodeord eller kryptere data og kræve løsesum for at låse op igen. Sidstnævnte er noget, der de senere år, er steget eksplosivt.

Hvordan fungerer det?

Computervira spreder sig automatisk fra computer til computer. Tidligere skete det oftest, når man delte programmer via lagringsmedier som disketter, men med internettet spredes de fleste vira gennem netværk og ved download af filer. Når en inficeret fil hentes og efterfølgende startes, aktiveres virussen.

En virus gemmer sig oftest sammen med andre eksisterende programmer (enten selvstændige programmer eller dele af styresystemet) og afvikler sig selv, når programmet startes.

Angreb og forsvar

De fleste computere er i dag udstyret med anti-virus-software, der holder øje med eksisterende vira og mønstre, der ligner disse. Det er derfor vigtigt at holde sin software opdateret. Desuden skal man være varsom med at downloade og installere programmer fra ukendte

kilder. Mange styresystemer tilbyder i dag central distribution af programmer, hvor der ofte er en bedre kontrol af programmer mod ting som for eksempel virus. Man skal derfor især være opmærksom, hvis man installerer programmer fra andre steder end disse kilder.

Historie

Verdens første computervirus hed "Creeper system" og var en selvreplikerende virus, der blev skabt som et eksperiment i 1971. Den fungerede ved at fylde harddisken, så computeren ikke længere fungerede. Den første virus til hjemmecomputere var "Brain", som blev skabt i 1986 som en kopibeskyttelse. Den fungerede ved at overskrive den såkaldte bootsektor på disketten, så computeren ikke kunne starte. To år senere kom den første internetvirus, ”The Morris”, som var et program, der skulle undersøge størrelsen af internettet ved at udnytte huller i forskellige protokoller, som for eksempel e-mail. Desværre var programmet dårligt programmeret og spredte sig derfor hurtigere end planlagt og endte med at inficere mere end 15.000 computere - eller stort set hele internettet dengang - på under et døgn.

Spillet

Bobby er en stor og klodset computervirus, der skader tre porte host modstanderen. Kortet er et aktionskort og kan derfor kun spilles, når det er din tur. Desuden er det et angrebskort, hvilket betyder, at man, når man er flere end 2 spillere, spiller kortet mod venstre (i urets retning). Når kortet er spillet, og skaden er givet, smides kortet i kortbunken.

BOBBYLINE (METAMORFISK VIRUS)

Bobbyline er et eksempel på en såkaldt metamorfisk computervirus. Det betyder, at virus, hver gang den inficerer en ny del af et computersystem, omskriver sig selv.

Hvordan fungerer det

En virus består typisk af en krypteret kode (payload), som, når den inficerede fil køres, dekrypteres og kører sit skadelige program, herunder inficering af yderligere filer. Den del af virus, der står for udpakningen, er den samme: Det er dén, som et antivirusprogram kan genkende. En mere avanceret form for virus, en såkaldt polymorfisk virus, sørger derfor for at skjule udpakningsdelen ved at ændre på denne ved hver ny inficering, men det kan virusprogrammet stadig genkende, når den dekrypteres, og den kan så slå alarm. Metamorfisk virus går trinnet videre ved at omskrive selve programmet gennem en slags metakode, så den ser ud på en helt ny måde, men stadig udfører den oprindelige funktion. Det betyder også, at en metamorfisk virus er meget stor og kompleks og har den største del af programmet til at udføre omskrivningen, mens selve virussens funktion fylder en mindre del.

Angreb og forsvar

Metamorfiske vira er svære men ikke umulige for antivirusprogrammer af genkende. Svagheden i metamorfisk virus er, at den skal analysere sig selv ved udpakning, og det betyder, at antivirusprogrammerne kan bruge samme teknikker til at finde virus, som virus bruger til at pakke sig selv ud med. For at beskytte sig mod avancerede vira som denne, er det dog ofte bedre med en sikkerhedspolitik, der sikrer systemerne mod overhovedet at blive inficerede.

BOBBYLINE (METAMORFISK VIRUS)

Historie

En af de tidligste eksempler på en metamorfisk virus er ”Zmist”, som blev skabt af den russiske programmør Z0mbie i starten af 2000-tallet. I 2016 blev en ransomware variant med navnet ”Virlock” opdaget, og man fandt ud af, at den havde en avanceret metamorfisk kodegenerator, der kunne skabe en ny unik udgave af sig selv for hver kopi af virussen.

Spillet

BobbyLine er en sofistikeret metamorfisk computervirus, der er dyr at bruge. Den koster 3 porte at spille, men skader til gengæld 5 af modstanderes porte. Kortet spilles som et aktionskort - altså på angriberens tur.

Et angreb der fungerer ved at bevidst at overbelaste den angrebne internetserver.

Hvordan fungerer det

DDoS står for Distributed Denial of Service, og det fungerer, ved at en lang række computere på samme tid sender forespørgsler til den samme server. Herved bliver serveren så belastet af forespørgsler, at den ikke er tilgængelig for den almindelige brug, eller måske endda går ned. Herved opleves det, som om den var blevet slukket.

Angreb og forsvar

Som med mange andre typer sikkerhedsudfordringer er det et konstant kapløb mellem angribere og forsvarere. I takt med at mange systemer hurtigt kan respondere ved at skalere sig selv op og lukke for specifikke adresser for forespørgsler, bliver angriberne også bedre til at lave specifikke angreb. De kan angribe bestemte protokoller eller udnytte endnu ikke lukkede sikkerhedshuller i serversystemerne. Heldigvis er DDoS primært noget, der rammer udbydere af hjemmeside, infrastruktur og andre systemer, som de færreste almindelige brugere behøver at bekymre sig med. Driver man selv hjemmesider eller andre internetbaserede tjenester, som er kritiske at have til at køre, er det bedste, man kan gøre, at sikre sig en god skalerbarhed og distribution af servere på forskellige netværk. Dette kan for eksempel opnås ved at anvende en udbyder med datacentre flere steder i verden.

Historie

Det første DDoS-angreb i historien fandt sted den 22. juli 1999, hvor 114 computere, der var inficeret med Trin00, angreb en computer på University of Minnesota. Det angrebne system blev så overbelastet, at

det ikke kunne svare på almindelige forespørgsler. Angrebet stod på i to dage, før det lykkedes at stoppe de inficerede maskiner, og var begyndelsen på DDoS som sikkerhedstrussel.

Spillet

Med dette kort laver man et midlertidigt angreb på modstanderens porte. Den angrebne skal lukke 5 porte. Portene åbnes igen, når runden er slut, medmindre den angrebne spiller har tabt. Kortet giver altså alene mening at spille, hvis man regner med, at resten af portene kan lukkes, eller man med dette kort lukker de sidste porte, den angrebne spiller har tilbage.

GLITCH

En glitch er en kortvarig fejl i systemet, som kun optræder i specielle tilfælde eller som automatisk udbedres eller ignoreres, så den er svær at identificere og rette.

Hvordan fungerer det

En glitch er noget, der ikke fungerer. Det kan være en mindre fejl (bug) i softwaren, som kun optræder i helt specielle tilfælde, eller en mindre hardware fejl, som kun sporadisk påvirker brugen (for eksempel en pixelfejl i en skærm). Ofte kan en glitch passere, uden at det opdages på det tidspunkt, den optræder, men senere kan den ses i en datafejl.

Angreb og forsvar

Glitches er som udgangspunkt ikke resultatet af angreb, men det kan være tilfældet. Man bør derfor være opmærksom, hvis et program begynder at opføre sig anderledes, eller der sker noget underligt, der ikke plejer at ske.

Historie

Udtrykket glitch kan spores tilbage til rumkapløbet i 1950'erne og handlede om mindre fejl i raketternes systemer, som ikke umiddelbart kunne afklares. Time Magazine definerede i 1965 udtrykket som værende "en rummands udtryk for irriterende forstyrrelser".

Spillet

En aktionskort som "glitcher" modstanderen, som derfor ikke kan spille kort fra hånden i en hel runde. Det betyder, at modstanderen hverken kan spille kort i sin egen runde, eller kan spille reaktionskort som reaktion på de kort, andre spillere spiller.

HAMSTER I KABLET

En hamster i kablet er et eksempel på, at ikke alle fejl i et computersystem skyldes fejl i software eller hardware – eller et angreb.

Hvordan fungerer det

Når der er fejl ved computeren, kan det skyldes både software, hardware eller angreb, men også at computeren ikke er forbundet ordentligt, eller der er opstået fejl i stik og kabler. Man bør ofte tjekke om alle kabler og forbindelser sidder ordentligt i stikkene, og at ingen af kablerne er beskadigede.

Historie

Fejl i computerprogrammer kaldes ofte for en bug. En bug henviser altså til en fejl, som får systemet til at gå ned eller kommer med et forkert resultat. Processen med at finde fejl kaldes "debugging", og mange softwaresystemer har forskellige egenskaber, der gør det lettere at finde og rette fejl under kørsel.

En historie fortæller at udtrykket "bug" (insekt) stammer fra 1947, hvor et insekt i et relæ fik en computer til at fejle. Udtrykket er oprindeligt et langt ældre ingeniørudtryk for fejl i systemer, måske endda fra før de blev elektriske. Fejlen i 1947 blev opdaget af en ingeniør, der kendte udtrykket og derfor gemte insektet med en note om, at det var det første eksempel på en rigtig "bug" i systemet. Historien viser, hvordan fejl i computersystemer kan skyldes ydre rammer og ikke selve computeren, ligesom hvis man har haft en hamster til at gnave i kablerne.

Spillet

Når man som en aktion spiller en hamster i kablet, forhindrer man modstanderen i at angribe i dennes næste tur. Modstanderen må altså fortsat spille kort, men ikke foretage angreb. Kortet skal blive liggende foran modstanderen, indtil dennes næste tur er overstået, hvorefter det ryger i bunken med brugte kort.

I AM NOT A ROBOT (CAPTCHA)

Der er ofte brug for systemer til at teste, om en bruger er en computer eller et menneske. Den meste udbredte metode kaldes CAPTCHA. Det er en forkortelse for *Completely Automated Public Turing test to tell Computers and Humans Apart* eller *Fuldautomatisk offentligt Turingtest der kan skelne mellem computere og mennesker*. Systemet bruges til at skelne for eksempel i forbindelse med brugeroprettelse, login og andre steder, hvor det er vigtigt at begrænse mulighederne, for at en computer gentager handlinger som for eksempel oprettelse af mailadresser, der kan misbruges til spam.

Hvordan fungerer det?

De første systemer bestod i høj grad af forvrængede billeder, hvor man så skulle gennemskue, hvad der i virkeligheden stod. Computere kunne ikke på dette tidspunkt ikke genkende tegn og bogstaver, der var forvrængede, lige så godt som mennesker.

Forsvar og angreb

I takt med at systemer til at beskytte mod robotter er blevet bedre, er der også oprustet på måden, man snyder en computer til at tro, at en robot er et menneske. Efterhånden som computere er blevet bedre til at løse denne type opgaver, er systemerne blevet udviklet til at bruge forskellige billeder, hvor man for eksempel skal genkende billeder med bestemte elementer. I dag fungerer systemerne i høj grad ved at benytte en masse forskellige brugerinput, herunder reaktionstider eller browserens historik i forhold til, hvor man kommer fra.

I AM NOT A ROBOT (CAPTCHA)

Historie

Behovet for at teste, om det er en ægte bruger eller et computerprogram, blev først for alvor stort i forbindelse med de mange tjenester, der opstod med udbredelsen af World Wide Web (eller internettet, som vi kender det i dag). CAPTCHA blev udviklet af Carnegie Mellon University i år 2000. Mange af de systemer, der validerer brugeren som menneske, har en sekundær funktion. De får brugerne til at hjælpe med vigtige data. For eksempel når man markerer, hvor på et billede der er biler, og disse data samtidig bruges til at træne computere gennem maskinlæring.

Spillet

Med kortet kan beskytte sig mod et angreb, men da det koster 4 porte at spille, er det dyrt og bør kun bruges mod voldsomme angreb. Kortet er et reaktionskort og kan spilles, når man udsættes for et angreb. Når kortet spilles fejler angrebet. Den, der angriber, skal stadig betale prisen, men den angrebne slipper med at betale 4 porte uanset angrebets styrke. Når kortet er spillet, og skaden givet, smides kortet i bunken med brugte kort.

MAN IN THE MIDDLE

Et *man-in-the-middle*-angreb er et angreb, hvor angriberen placerer sig mellem to enheder og udgiver sig for at være begge enheder, så de hver især tror, at de taler med den anden enhed.

Hvordan fungerer det

Ved et *man-in-the-middle*-angreb vil al kommunikation mellem de to enheder, der er forbundet via angriberen, kunne gemmes og manipuleres af angriberen. Det kan for eksempel ske ved at udgive sig for at være et offentlig wifi-netværk med næsten samme navn som det rigtige eller med en større sendestyrke. Hvis man således har sat sig om mellem en computer og internettet, vil man kunne opfange alle forespørgsler og svar, der sendes via nettet. Disse kan angriberen så enten gemme en kopi af eller endda ændre, inden de sendes videre.

Angreb og forsvar

Med de mange gratis wifi-hotspots er det let at opsætte og misbruge dem til at lave *et man-in-the-middle*-angreb. Man bør derfor altid være forsigtig, når man benytter fremmede netværk, især til sensitive informationer som arbejdsmailen eller bankkontoen. Heldigvis er der flere gode måder at beskytte sig på. Man kan for eksempel anvende et Virtuelt Privat Netværk (VPN) eller kun at besøge sider på internettet, der benytter HTTPS. I dag benytter de fleste webbrowsere HTTPS som standard og giver en alarm, hvis en webside kun understøtter HTTP.

Begge metoder beskytter ikke fuldstændigt mod misbrug af manden i midten, men gør det til et meget større arbejde at få noget ud af data, og man kan derfor håbe, at angriberen giver op og finder et lettere mål.

MAN IN THE MIDDLE

Historie

Ideen om at placere sig mellem afsender og modtager i en kommunikation er ikke ny. Metoder til at undgå, at for eksempel skrevne beskeder blev læst af de forkerte, har været kendt siden antikken, gemmen både kryptering og forsegling. I computersammenhænge stammer udtrykket helt tilbage fra slutningen af 1970'erne, men udfordringen med denne type angreb er først for alvor blevet udbredt sammen med internettets udbredelse op gennem 1990'erne.

Spillet

I hackerspillet er *Man in the Middle* et reaktionskort, man kan spille, når man bliver angrebet. Kortet bytter om på skade og pris på et angrebskort, spillet af en modstander.

PHISHING MAIL

Phishing er en metode, hvor angriberen forsøger at franarre brugere oplysninger, for eksempel kodeord, kreditkort eller andre brugbare informationer. Angrebet sker ved, at angriberen gennem en henvendelse forsøger at lokke offeret til at besøge en falsk hjemmeside, få dem til at afvikle malware eller måske svare direkte med person- og bankoplysninger eller få overført penge

Hvordan fungerer det

Phishing fungerer ved, at man, for eksempel gennem en e-mail, en besked på Messenger eller tilsvarende beskedtjeneste, får tilsendt en besked. Beskedens formål er at lokke brugeren til at udføre en eller flere handlinger, som angriberen kan bruge til sit formål. Det kan være at klikke på et link, som ligner for eksempel banken, Skat eller en tilsvarende autoritet, og hvor brugeren skal indtaste loginoplysninger, bankkonto, kreditkortnummer eller andre oplysninger, som angriberen er efter. Det kan også være, at angriberen forsøger, at få brugeren til at afvikle malware, der f.eks. kan kryptere computeren, så angriberen kan kræve en løsesum for at frigive dem igen. Endelig kan det også være målet, at få brugeren til at svare og sende kreditkortoplysninger eller andre data om sig selv.

Angreb og forsvar

Phishingforsøg var i starten ret kluntet udført. De beskeder, der blev sendt, var lette at genkende som værende mærkelige gennem dårlig stavning, opsætning og forkerte logoer og skrifttyper. Phishing er i stigende grad blevet mere sofistikeret. Udover at være bedre udført, ser man også ofte, at de udnytter bestemte tider på året. For eksempel ved den tid, hvor man indberetter sin selvangivelse, så der kommer en mail, der ser ud til at komme fra Skat. Man bør derfor altid spørge sig selv, om afsenderen ville sende en mail, og bede om

de ønskede oplysninger. For eksempel sender Skat aldrig en mail om, at du skal indtaste dit kreditkortnummer, da de bruger din såkaldte NemKonto til at udbetale penge til borgere. Man kan også kigge efter tegn i selve beskeden og ikke mindst de links, der er medsendte. Er du for eksempel mistroisk over for en mail fra din bank, så skriv selv bankens hjemmesideadresse i browseren fremfor at klikke på linket i en mail, eller brug andre metoder for at validere afsenderen ved f.eks. at ringe eller maile til vedkommende.

Historie

Selve udtrykket phishing henviser til, at man fisker efter oplysninger. Det er en almindelig tradition i hackermiljøer at udskifte f med ph. Ideen med at udgive sig for at være en anden og få penge eller oplysninger på den måde er ikke ny i den fysiske verden. Som internetfænomen opstod det 1990'erne på den store nordamerikanske udbyder AOL. Her udgav en gruppe hackere sig for at være AOL-ansatte i mails til forskellige kunder for at franarre dem kreditkortsoplysninger.

Spillet

Når man på sin tur spiller Phishing, må man kigge bunken med brugte kort igennem og vælge et kort, man gerne vil trække op på hånden.

POWERBANK

En powerbank er en elektronisk enhed, der kan overføre en mængde strøm til at oplade andre batteridrevne enheder.

Powerbanken er så udstyret med to stik. En indgang til at lade op og en udgang til af lade andre apparater lade op via powerbanken. De fleste powerbanks er i dag udstyret med USB-stik både til strøm den ene vej og til strøm den anden vej.

Som med andet elektronik, der forbindes via usb, skal man være opmærksom på, at enheden er det, den udgiver sig for at være. For eksempel hvor og hvordan man har fået adgang til den.

Spillet

Kortet er både et reaktionskort og et aktionskort og kan altså spilles når som helst. Det er gratis at spille. Det genoplader dit system og lader dig åbne 3 porte. Kortet kan spilles som et reaktionskort for eksempel i forbindelse med et angreb, hvor man mister porte. Det kan også spilles som et aktionskort, for eksempel lige inden man selv angriber for at have porte nok til at gennemføre angrebet.

SHITSTORM

Shitstorm dækker over en sag på sociale medier, der giver en stor mængde negativ omtale eller dårlige anmeldelser.

Hvordan fungerer det

En shitstorm er kendetegnet ved, at en person eller en virksomhed får en så stor mængde negativ omtale, at det ikke er muligt at kontrollere eller håndtere, og man dermed mister kontrollen over situationen. Det kan være meget ubehageligt som enkeltperson og kan føre til store personlige og endda økonomiske konsekvenser, ligesom det kan være skadeligt for virksomheders image og bundlinje.

Angreb og forsvar

En shitstorm er som sådan ikke et angreb på sikkerheden, men der er eksempler på grupper af modstandere af for eksempel en virksomhed, som har arbejdet på at opbygge en shitstorm. Den bedste måde at undgå, at negativ omtale udvikler sig til en decideret shitstorm, er at følge med på de forskellige sociale medier og have en klar strategi for, hvordan man håndterer negativ omtale, så den ikke får lov at vokse sig uhåndterlig.

Historie

Udtrykket shitstorm er et amerikansk slangudtryk for en skandale eller katastrofal kontrovers, der stammer helt tilbage fra 1940'erne. Som udtryk for, at det går helt galt på internettet, er begrebet dog kommet til os fra tysk, hvor det er blevet brugt siden starten af 2010'erne og blev optaget i den tyske retskrivningsordbog Duden i 2013 med den samme betydning, som vi nu har på dansk.

Spillet

I hackerspillet er en shitstorm et aktionskort, man kan spille mod en modstander efter eget valg. Man kan således i spil med flere end to spillere selv vælge, hvem angrebet skal rettes mod.

TO-FAKTOR-GODKENDELSE

To-faktor-godkendelse handler om, at man skal igennem to (adskilte) måder at identificere sig på for at få adgang til et system. Det kan være kombinationen af noget, man *ved* (for eksempel en kode) og noget, man *har* (for eksempel en nøgle).

Hvordan fungerer det

Der findes en række forskellige måder at lave to-faktor-godkendelse på. De mest udbredte er i dag en kombination af et almindeligt brugernavn og kodeord, som efterfølgende kræver en bekræftelse via et eksternt system. Denne bekræftelse kan for eksempel være et nummer sendt til telefonen, et engangskode fra et kodekort hos brugeren (som det kendes fra NemID), en hardware nøglegenerator eller en autentificeringsapp fra en udbyder som Google eller Microsoft. Der kan også være tale om biometrisk identifikation gennem fingeraftryk, øjets iris, stemme eller andre mønstre, der kan genkendes som unikke.

Angreb og forsvar

Identifikation alene med brugernavn og kodeord er usikker, hvis man for eksempel har et for simpelt kodeord eller har brugt samme kodeord flere steder. Med to-faktor-godkendelse tages en stor del af denne usikkerhed ud, ved at man skal igennem endnu et sikkerhedstjek. En af de mest udbredte former er, at man modtager en kode på telefonen. Desværre er telefonsystemet ikke sikkert, og det anses derfor som en usikker metode i sammenligning med andre metoder. Man opnår derfor større sikkerhed ved at anvende en kodegenerator - enten en app, der med en algoritme hele tiden genererer nye koder, eller en fysisk enhed, der fungerer på samme måde. Man skal ikke overlade hele sin sikkerhed til to-faktor-

godkendelse, men det er et rigtig godt supplement til brugen af sikre (lange og unikke) kodeord og andre gode vaner omkring login.

Historie

Brugen af kodeord til computersystemer strækker sig helt tilbage til de sene 1950'ere. Først med internettets udbredelse gennem World Wide Web blev der for alvor brug for bedre sikkerhed end kodeord. Allerede omkring år 2000 begyndte man at se små hardwarebaserede nøglegeneratorer på størrelse med et usb-stik som to-faktor-login. Problemet med disse dimser er, at man skal have en dims per hjemmeside eller system, og at de desuden er forholdsvis dyre at fremstille. Det er derfor først med brugen af mobiltelefoner, dels gennem tilsendte koder over sms og ikke mindst med fremkomsten af egentlige autentificerings-apps, at to-faktor-godkendelse er blevet udbredt.

Spillet

Når man spiller to-faktor-godkendelse, lægger man det foran sig. I resten af spillet vil man, hver gang man har tur, få lov til at åbne yderligere +1 port. Man kan godt have flere af dette kort liggende foran sig på samme tid.

TROJANSK HEST

En trojansk hest er en type virus. Den er navngivet efter den krigslist, som Odysseus udtænkte til at indtage Troja i antikkens Grækenland. I Troja gemte Odysseus og hans mænd sig i en kæmpe træhest, som indbyggerne i Troja trak ind i byen. Herfra kunne de så om natten snige sig ud og vinde over byens forsvarere. I sikkerhedssammenhænge betegner en trojansk hest et stykke ondsindet software, som brugeren lokkes til selv at installere, idet det er kamufleret som brugbar software.

Hvordan fungerer det

En trojansk hest er en type virus, som, når den rammer systemet, åbner en bagdør til offerets computer. Bagdøren kan angriberen så bruge til at trænge ind bag computerens sikkerhedssystemer. Når først angriberen har fået bagdøren på plads, kan angriberen misbruge sin adgang. Det kan for eksempel være til at samle informationer om det ramte system og dets brugere. Det kan også være ved at udnytte det ramte system til at foretage opgaver for angriberen, for eksempel ved at indgå i et såkaldt botnet eller til at fremstille bitcoins.

Angreb og forsvar

Trojanske heste er den absolut mest udbredte form for malware, da de inficerede systemer kan indgå i botnets og således misbruges af angriberen til at foretage andre angreb. De første trojanske heste var ikke så gode til at skjule deres handlinger i computersystemernes logfiler over internettrafik, men de er blevet bedre til at slette sporene efter sig selv. Den bedste måde at beskytte sig mod trojanske heste er kun at hente og installere software fra sikre kilder og i øvrigt sørge for opdateret sikkerhedssoftware.

TROJANSK HEST

Historie

Det første program, der af de fleste ses som en trojansk hest, var programmet ANIMAL fra 1975. ANIMAL bestod af et simpelt spil, der samtidigt kopierede sig selv til et fællesdrev. Herfra kunne andre brugere så også installere det, og hermed kunne den spredes. Det første eksempel på en farlig udgave var AIDS Trojan fra 1989. Denne virus gjorde først noget, når computersystemet havde været slukket 90 gange. Herefter krypterede den hele systemet og gav brugeren en besked om at sende penge til en konto i Panama for at få en nøgle til at låse systemet op igen. I dag findes der også trojanske heste til mobiltelefoner, så også her skal man være forsigtig - især hvis man bruger andre kilder til programmer end de officielle appbutikker.

Spillet

I hackerspillet giver en trojansk hest ikke selv nogen skade, men gør næste angreb på den ramte spiller porte meget værre. Det betyder, at næste angrib giver dobbelt skade. Kortet skal blive liggende foran modstanderen indtil næste angreb. Hvis der spilles mere end et kort af denne type, giver det kun ekstra skade svarende til angrebet for hvert kort, der spilles. Har en spiller således to trojanske heste liggende foran sig og bliver ramt af et kort, der lukker 3 porte, vil angrebet lukke 2 x 3 porte + 3 porte: Altså i alt 9 porte.

USB-TROLDMAND

Et usb-angreb er et angreb, der udløses af, at man sætter et skadeligt usb-stik i computeren. Det kan være et usb-stik, der inficerer computeren med virus, får den til at udføre uønskede handlinger eller decideret ødelægger hardware i computeren

Hvordan fungerer det

Der findes en lang række forskellige angreb via usb. Det simpleste er, hvor der simpelthen ligger en (eller flere) virusinficerede filer på et usb-drev. Der kan også være tale om usb-stik, som computeren tror er et tastatur, og som sender en række kommandoer, som computeren udfører. Endelig er der også angreb, hvor et skadeligt usb-stik indeholder en kondensator, der tager strøm fra computeren, og efter et par sekunder leverer den tilbage som et stød. Dette vil, hvis computeren ikke er tilstrækkeligt beskyttet (på hardwareniveau), få hele computeren til at brænde sammen.

Angreb og forsvar

Da computere først fik cd-rom-drev og siden usb-stik, var mange styresystemer sat op til at afvikle programmer fra disse automatisk. Det betød, at man kunne få programmer - også skadelige - til at starte af sig selv, når disken eller drevet blev sat i. Dette beskytter de fleste systemer mod i dag. Usb har dog stadig den usikkerhed, at man altid skal kunne sætte et tastatur og en mus til computeren. Det har hackere udnyttet, så man i dag kan lave usb-stik, der genkendes som et tastatur af computeren, når det sættes i, og hvor angriberen på forhånd har "programmeret" en række tastetryk. Det kan for eksempel være kommandoer, der kopierer eller starter et program på en anden del af usb-stikket eller starter browseren og besøger en bestemt hjemmeside. Det er derfor vigtigt, at man aldrig sætter usb-

stik i sin computer, som man ikke ved, hvor kommer fra, og at man i øvrigt altid har opdateret sin software.

Historie

Brugen af usb-medier til at udbrede virusinficerede filer har været kendt lige så længe som brugen af usb-medier. De første deciderede usb-angreb kom i 2010 i forbindelse med et stykke hardware, hvor man igennem en mikrocontroller - et såkaldt Teensy-board - kunne programmere et usb-stik, som agerede tastatur og sendte en række forprogrammerede tastetryk. Det blev udviklet til at hjælpe administratorer, der skulle udføre og gentage samme opgave på mange computere. Hackere var dog ikke sene til at udnytte idéen til at sprede malware.

Spillet

I spillet giver usb-troldmanden skade og lukker fire porte, når kortet spilles. Det er et aktionskort, som kun kan spilles, når angriberen har tur.

PORTE

I et operativsystem er en port en logisk konstruktion, der identificerer en specifik proces eller type af netværksservice. En port er identificeret med portnummer, og der er specifikke porte til forskellige typer af kommunikation eller dataudveksling.

Hvordan fungerer det

Når man skal kommunikere over et netværk, har man brug for at vide, både hvem man skal kommunikere med og hvordan. Denne kommunikation foregår i de fleste tilfælde over internetprotokollen og betyder, at man skal kende IP-adressen på den, man skal kommunikere med.

Udover IP-adressen skal man også vide, hvilken port man skal kommunikere på. Samlet kalder man protokol, ip-adresse og portnummer for en socket. Ved at anvende specifikke og velkendte portnumre til bestemte services kan man have systemer til at stå og lytte efter forespørgsler på disse specifikke porte og være klar til at svare.

For eksempel kan man se på, hvad der sker, når man indtaster www.hackerspillet.dk i browserens adressefelt:

Først vil browseren slå DNS-adressen op, så den kan få IP-adressen, som www.hackerspillet.dk befinder sig på. Derefter vil den forsøge at skabe en TCP-forbindelse til IP-adressen på port 80, da der er tale om en www-server, og den derfor vil forsøge med http-protokollen. Serveren på den kaldte adresse vil, hvis forbindelse oprettes, levere et en hjemmeside i HTML eller XML.

Spillet

I spillet er porte en måde at tale om point, liv eller energi. Alle handlinger koster porte, og ligeledes kan andres handlinger (angreb) koste porte. Man bruger portoversigten til at have overblik over, hvor mange porte man stadig har åbne. De enkelte porte har ikke en særlig funktion i forhold til kortene i standardspillet, men det kan jo være, at nogen udvikler nye kort, der angriber eller måske permanent lukker bestemte porte. Følgende porte er med i Hackerspillets portoversigt:

- 20 FTP (File Transfer Protocol) datatrafik
- 21 FTP (File Transfer Protocol) kontrol
- 22 SSH (Secure Shell)
- 23 TELNET
- 25 SMTP (Simple Mail Transfer Protocol)
- 53 DNS (Domain Name System)
- 67 DHCP (Dynamic Host Configuration Protocol)
- 68 DHCP (Dynamic Host Configuration Protocol)
- 80 HTTP (HyperText Transfer Protocol)
- 110 POP3 (Post Office Protocol Version 3)
- 143 IMAP (Internet Message Access Protocol)
- 194 IRC (Internet Relay Chat)
- 213 IPX (Internetwork Packet eXchange)
- 427 SLP (Service Location Protocol)
- 433 NNSP (Network News Transfer Protocol)
- 443 HTTPS (HTTP med Secure Socket Layer)
- 444 SNPP (Simple Network Paging Protocol)
- 666 Doom
- 989 FTPS (FTP med Secure Socket Layer) datatrafik
- 990 FTPS (FTP med Secure Socket Layer) kontrol