STAND VAN ZAKEN:

BROADCAST CYBERSECURITY

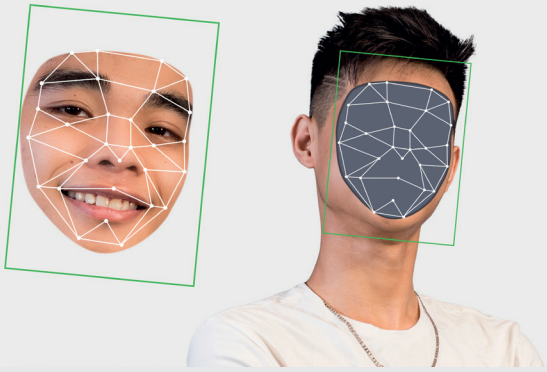
Technologie verandert alles binnen de broadcastindustrie. Van ENG en storytelling tot distributie over IP en de gevoeligheid voor cybercrime. Dankzij de enorm toegenomen connectivity via internet en mobiele media voor het afleveren van content in elke gewenste vorm, tijd en plaats om de klant zo optimaal mogelijk streaming en on demand te voorzien, gaan hiermee ook de poorten open voor op geld beluste criminelen.

Door: Ulco Schuurmans

Vrijwel elke vorm van cybercriminaliteit die bedrijven en burgers teistert betreedt nu ook de 'goudmijn' van de media-industrie en broadcasting. Fishing, website spoofing, het stelen van content en OTT-inkomsten, ransomware, (deep) fakes en het platleggen van services. Noem het maar op en het heeft inmiddels al op grote schaal plaatsgevonden. De winsten voor de criminelen zijn relatief gezien gigantisch. Dat verklaart waarom cybercriminaliteit inmiddels de vorm van de perfecte digitale storm heeft aangenomen en vrijwel overal in de industrie rampspoed teweegbrengt. Dat betekent uit lijfsbehoud beveiligen, security en nog meer security voor broadcast en contentgevoelige media!

TRENDS

Recent onderzoek van de EBU onthulde dat broadcasters en de media-industrie behoorlijk kwetsbaar zijn



NEPNIEUWS, DEEP FAKING EN VOICE CLONING

Met *disruption in mind* strooien kwaadwillende groepen en malafide infuencers en zelfs bepaalde regimes rijkelijk met vals beeld- en geluidsmateriaal op omroep- en distributienetwerken. Zo creëren deze figuren een ware infocalyps van misinformatie. Volgens Forbes momenteel een uiterst serieuze dreiging! Fake news valt zo door een achterdeurtje naar binnen het IP-netwerk te manoeuvreren. En mensen trappen er onder het vertrouwde zender- of weblogo gewoon in.

(Deep)faking is een flinke graad erger. Het bewust aanpassen c.q. vervalsen van bestaande content of het namaken daarvan. Technieken waarvan de postproduction dankbaar gebruik maakt om landschappen, achtergronden, objecten en personen met de grafische computer aan te passen zijn heel wel bruikbaar voor misleiding. De makers kunnen zowel op jouw systemen inbreken (via het IP-netwerk of the Cloud) bij de postproduction of downstreaming en ook elders gefabriceerde rotzooi importeren.

Zorgwekkend is dat vrijwel iedereen bij de benodigde apps en hardware (een iPhone is al genoeg) kan. Wat bijvoorbeeld te denken van Deepnude (voor freaks), AI-systemen die op basis van teksten gefingeerde krantenkoppen/artikelen fabriceert (GPT2 van OpenAI) en generative adversarial networks (GAN-systemen) waarbij AI-netwerken elkaar beconcurreren wie de beste (nep-)output naar buiten brengt. GANs hebben realistische menselijke verbeeldingskracht en zijn daarom interessant voor storytelling producties bij contentnetwerken. Maar als die story's nu eens de verkeerde kant opgaan? Wie houdt de veiligheid en waarheid in de gaten? En vervangt GPT2 straks de journalistiek? Het herkennen van deep fake-bewerkingen is lastig, maar wel goed mogelijk.

Een andere tak van sport vormt voice cloning: Het gebruik van software om een synthetisch acceptabele kopie van iemands stem te maken. Dat gaat het stuk verder dan knip- en plakwerk met echte stemfragmenten. Je kunt mensen echt van alles naar waarheid klinkend laten zeggen. Dit compleet met menselijke emoties en stemmingen. Natuurlijk leuk voor animatiefilms en zo, maar ronduit een bedreiging als men zo realistisch politici en omroepmedewerkers nadoet. Om het over binnendringen met spraakherkenning nog maar niet hebben.

Soft- en hardware

Bij de bescherming door software zijn een virusscanner en fishing-blokkade alleen natuurlijk niet voldoende. Daar komen nog vergaande toegangscontroles, het continu monitoren van netwerkactiviteiten op betrouwbaarheid en live stromen en het afwenden van blokkade-aanvallen bij. Houd verder alles up-to-date bij de besturingssoftware apps en firmware. Een andere optie betreft het gebruik van een versterkt besturingssysteem (OS), bijvoorbeeld een speciale Windows-versie. Let met name op de kwetsbaarheid van IOT-apparaten zoals smart-tv's. Bij een gedetecteerde aanval via rapid respons zo snel mogelijk kwetsbare systemen afsluiten en/of kritische processen omleiden.

Bij de hardware gaat het doorgaans om combinaties van AV-servers en IP-devices met ingebouwde extra security software en back-up-mogelijkheden. Bijvoorbeeld antivirus, toegangscontrole en redundant opslag van kopieën. O.a. Stryme verkoopt dergelijke complete pakketten.

voor cyberaanvallen. Vaak is de beveiliging onvoldoende op orde en is er nog maar weinig echt over nagedacht. Daar komt nog bij dat de productie- en distributie-industrie grootschalig bezig is om over te schakelen naar nieuwe AV over IP-technieken. Dat maakt het allemaal kwetsbaar voor cyberbedreigingen en menig bedrijf viel daar inmiddels al aan ten prooi.

Complicerend is dat behalve de traditionele hacks de broadcast-industrie extra gevoelig blijkt voor content piracy, het afromen en skimming van OTT-winsten en het treffen van de privacy van haar klanten/afnemers door hackers. Om het over nepnieuws en deep faking nog maar niet te hebben. "Gone are the days when broadcast equipment consisted of custom software running on dedicated hardware", zo luidt één van de kernproblemen. D.w.z. dat het van overzichtelijke kant-en-klare robuuste applicaties naar netwerken van alles en nog wat overal ter wereld is gegaan. En dat maakt beschermen tegen cybercriminaliteit behoorlijk lastig.

Er valt gelukkig ook goed nieuws te melden. Broadcasters scoren goed bij de beveiliging op het gebied van unpatched software en remote access. De meeste andere problemen zijn met de nodige aandacht en een goede strategie afdoende te fixen. Zwaktes liggen nog bij de juiste wijze van encryptie (33,5% van de gevallen), overbodige kwetsbaar makende features (26,5%), inlogbeveiliging (13,6%), slecht beveiligde interfaces en IOT-equipment (13%), gevolgd door ransomware (bescherming tegen en back-ups) en (D)Dos-aanvallen. Overall blijkt de menselijke factor (onoplettend, slordig, vertrouwend op) voor 80% aan de basis der cybercrimegevallen te liggen.

In ieder geval nemen de aanvallen op broadcastsystemen stormenderhand toe, omdat daar financieel en politiek (beïnvloeding door staatshackers) en door bedenkelijke actiegroepen (complotdenkers e.d.) veel te halen valt. In Nederland zijn er momenteel tegen de vijfduizend fraudemeldingen per dag. Relatief is de hevigheid waarmee operationele technieken momenteel door cybercriminelen onder vuur worden genomen. Professionele criminele teams vallen vitale infrastructuren aan, veelal met malware. Zij vinden de zwakke plekken binnen bedrijven. De hele keten van de desbetreffende corebusiness en eigen netwerken >

en de toeleveranciers, distributeurs en aangesloten cliënten zijn het cyberhaasje. Dat maakt cybersecurity, ook bij broadcast, tot de hoogste prioriteit!

AANVALLEN OP DE MEDIA

Helaas zijn er inmiddels al tal van voorbeelden van cyberaanvallen op de media en broadcasters. Geruchtmakend waren de hack van TV5 Monde (een zogenaamd Trojaans paard legde het zendernetwerk plat) in 2015 en het skimmen (financieel afromen en datadiefstal cliënten) van de e-commerce websites van de Warner Bros Musicgroup in 2020. Canon kreeg in 2020 ransomware en grootschalige (10 TB) datadiefstal over zich heen en al in 2014 werd Sony Pictures breed gehacked met een Service Message Block (SM) wormtool door Noord-Korea. Ook viel in 2014 de Australische netwerkzender ABC News 24 ten prooi aan massieve blocking. En Channel 9 ontsprong in maart van dit jaar de dans van een cyberattack niet. Dit jaar werden ook in de VS diverse nieuwsstations (deels) lam gelegd door aanvallen met ransomware. Het is nog wachten op een grote klap in Nederland.

UITDAGING

Naast de switch van SDI naar IP en de convergentie van broadcast en IT vormt broadcast media security een van de drie grootste uitdagingen van dit decennium. Ruwweg kent deze broadcast security twee categorieën: allereerst de Informatie Technologie van de betrokken onderneming en daarnaast de content generation en broadcastchain zelf. Bij de IT van de (media-)onderneming gaat het zoals gebruikelijk om de beveiliging van de e-mail, dataservers, netwerkapplicaties en toegepaste software. Hacking in het eigen IT-systeem kan leiden tot het platleggen van systemen, informatiediefstal en ronduit sabotage. Daar komt de trend van ransomware nog bij. Een inbraak op jouw systeem kan ook nog eens de daarmee verbonden klanten schaden. Van andere orde zijn de toegenomen risico's bij het thuis en op afstand (groeps)werken. Dat breidt de benodigde security uit tot alle aangesloten werkplekken.

Diefstal van content (piracy), het afromen van OTT-inkomsten en het manipuleren of lamleggen van informatiestromen naar clientèle vormen een toenemende bron van zorg. Ook kunnen cybercriminelen jouw klanten en online medewerkers hacken via de online verbindingen. Een tweede onderscheid is die in hardware- en softwarematige bescherming. Dikwijls werken beiden ook samen bij broadcast en media security. Een belangrijke nieuw loot is kunstmatige intelligentie. AI kan middels patroonherkenning en slimme identificatie gemakkelijk hackpogingen herkennen. Omgekeerd kunnen helaas criminelen AI inzetten om de broadcastbeveiliging te kraken of te omzeilen. >

Livestream en opnamestudio Roosendaal

Om te bouwen naar eigen identiteit en wensen, multi inzetbaar.

DUTCHMULTICAM®

RELIGHT GROUP BV

Studio is per dagdeel te huur, als complete setup inclusief camera's, regie, audio en licht, maar ook leeg.
Liever op locatie? Geen probleem.

Info:
Martijn Satter - Relight Group BV - Martijn@relight.nl - 06 543 110 44
John Huijbregts - DutchMulticam - John@dutchmulticam.nl - 06 247 297 28

WAAR GAAT HET OM?

De meest voorkomende typen cybercriminaliteit op een rij. Allereerst Phishing Scams. Het hengelen naar toegang tot systemen en beveiligingsdata maakt circa 91% van alle cybercrime uit. Het vissen betreft zowel individuele personen als websites en complete netwerken. Een variant is website spoofing, het vervalsen van identiteitskenmerken om toegang te krijgen om anderen naar jouw weblocatie te lokken. Het plaatsen van kwaadwillende programma's wordt malware injection genoemd. Bijvoorbeeld het gebruik van Trojaanse paarden.

Dan is er ransomware, het gijzelen van computerservers en netwerken heeft grootse vormen aangenomen. Menige omroep en provider kan daarvan helaas meepraten.

Het hacken via IOT-apparaten en het stelen bij OTT-diensten (o.a. via skimmingprocedures) dan. Ook de complete content wordt regelmatig gestolen via cyberpiracy.

En dan heb je nog sabotage. De laatste tijd zijn (D)Dos-aanvallen weer een trend. Dat vindt de kijker, e-sporter of e-gamers beslist niet leuk als de streamingverbindingen massaal worden lamgelegd. Hetzelfde geldt voor Twitter-bombardementen.

Faking en deep faking vormt een ware plaag. Wat kan je als lezers van het nieuws en het bekijken van programma's nu wel vertrouwen of niet? Je wordt tijdens het kijken en/of luisteren met fake-news en gemanipuleerde content gewoon bedonderd waar je bij staat.

Als laatste item de beveiliging van het gebouw of de opnamelocatie. Daarbij gaat het met name om camera-surveillance en persoonsherkenning met toegangscontrole. Helaas worden beveiligingscamera's en toegangspoortjes regelmatig ook zelf gehackt.

BEZORGDHEID

De broadcast- en media-industrie kent verschillende productie- en distributieketens. Een mix van live en vooraf opgenomen content, productie op verschillende plaatsen, tal van verschillende bewerkings- en postproductieplatforms, distributie (rooting en MAM) op multiple platforms en een grote variëteit aan interlinking broadcast chains. Allen lopen een serieus risico bij cybercriminele bedoelingen.

Een aantal keten-overwegingen. Als eerste onder embargo en vertrouwelijk. Dat vormt met name een probleem bij vooraf opgenomen programma's, series en filmproducties. Het zou niet de eerste keer zijn dat een blockbuster van te voren al gejat en op internet verspreid werd. Masters en kopieën behoren in een veilige digitale kluis met geautoriseerde toegang. Bij live uitzendingen speelt dit minder, maar het komt regelmatig voor dat het niet wenselijk is dat iedereen op het IP-netwerk kan meekijken. Access management voor pay-tv en betaalde sport- of gamekanalen is gewoon een must.

Integriteit en beschikbaarheid zijn eveneens ketengevoelig. De goede naam en betrouwbaarheid van broadcasters en mediadistribiteurs hangt af van een betrouwbare en op het gewenste moment ook beschikbare content. Er is veel te doen over het knoeien met (nieuws-)content. Fake-news, het namaken van programma's (faking) en deep faking waarbij het aanzien en de reputatie van de betrokkenen geschaad kunnen worden. Het beïnvloeden van opinies en verkiezingen of het ongeloofwaardig maken van tegenstanders bijvoorbeeld. Wie kan er ongewenst bij de content production en distribution komen?

Je kunt kijkers en afnemers niet bozer maken dan wanneer de uitzending van een film of sportwedstrijd plotseling wegvalt. Kwaadwillenden kunnen met een Denial of Service aanval (DoS) en Distributed Denial of Service (DDoS) de complete streaming dienstverlening platleggen. De mediaservers raken overbelast. En met ransomware zetten de cybercriminelen het gehele contentarchief op slot. >

Het stelen van live OTT-streams

Het live stelen van nieuwsuitzendingen, shows, sport- en muziekevenementen neemt grote vormen aan. Softwarematig gezien (capture en rerouting) is dat jatten niet eens zo moeilijk. Winstgevend is het wel bij koppeling aan reclames bij vertoning op het eigen platform en het verwerven van klantgegevens. De abonnementloze cord cutters zien en horen het allemaal graag gratis en nemen de reclames (en vaak ongeziene) dataverga-ring voor lief. De legitieme providers zijn dan de klos.

Zonder continue monitoring van de distributielijnen op het netwerk, watermerken, sluitende DRM en goede afspraken over content delivery door derde partijen staan de sluizen voor deze vorm van contentpiracy wijd open. Het opzetten van een eigen Content Delivery Netwerk (CDM) scheelt een hoop zorgen.

Camera's en toegangspoortjes

Het beveiligen van de eigen gebouwen en studio's met beveiligingscamera's en toegangspoortjes is onmisbaar bij broadcast-security. Zie en monitor wat er gebeurt. Detecteer onregelmatigheden. Houd de toegangscontroles op niveau en voer regelmatig systeemtesten uit.

Wees er op bedacht dat bewakingscamera's op het netwerk kunnen worden overgenomen door criminelen. Beveilig het systeem daartegen.

Efficiënte cybersecurity en de bijbehorende strategie is gewoon een must voor de broadcast en mediaproductie & distributie-industrie. Anders gaat dat straks een hoop Bitcoins, vervolgschade en imagoverlies kosten. Hoewel natuurlijk niet alles te voorkomen valt, telt een gewaarschuwd broadcaster in deze wel voor drie. En zorg als het dan toch misgaat voor voldoende back-ups en reservesystemen. Als laatste de journalistieke waarheid, die mag niet ten prooi vallen aan de infocalyps.

BEGIN AAN DE BASIS

Je hoeft zeker niet zelf het beveiligingswiel te gaan uitvinden. Er zijn voldoende protocollen en richtlijnen voor de basisbeveiliging voor broadcasting en mediadistributie beschikbaar. Van begin tot het einde van de keten, de betrokken mensen (medewerkers en klanten) en technologie. Wij noemen: NIST Cybersecurity Framework, COBIT (Control Objective over Information and related Technology) of de ISO 27K serie. Die voldoen voor de doorsnee bedrijfsvoering. Speciaal voor de Broadcast Media cybersecurity zijn er standaards zoals het DPP Committed to Security Programme, de CDSA Content Protection & Security Standard en de MPAA Content Security Best Practices. De EBU publiceert een aantal aanbevelingen specifiek gericht op broadcast & mediabeveiliging zoals Vulnerability Management (R160), Cloud Security for Media (R146) en Mitigation of Ransomware and Malware Attacks (R145). Kijk ook eens bij Digital Production Partnership (DPP) voor het 'Committed to Security'.

BEVEILIG CONTENT EN MENSEN

Het beschermen van content tegen cyber- en andere criminaliteit kent diverse aspecten. Eentje waar vaak niet zo snel aan gedacht wordt is de bescherming van het eigen merk. Gaat er een crimineel met de brandnaam of onder jouw broadcastvlag aan de slag, dan valt regelmatig de ellende niet te overzien. Fake-news en niet geautoriseerde publicaties zijn de pest. Daarnaast maken verhalen over lekken bij interne communicatie en bedrijfsgeheimen de naamsbekendheid er ook niet beter op.

Content (on line) delivery op maat naar de klant is momenteel tot een ware kunst verheven. Dit compleet met ondersteuning door data-analyse en AI. Hier dreigt het hackgevaar van diefstal van de persoonlijke data van de cliënt bij aflevering en OTT-afrekening.

Vergeet zeker niet om de eigen werknemers te beschermen. Dat betreft niet alleen hun persoonlijke gegevens, maar ook waar zij wonen en werken. Met de huidige vijandige bejegening van journalisten door bepaalde partijen en criminelen is het onwenselijk dat er bekend is waar zij precies zitten en opereren. Het is geenszins de bedoeling dat een mojo-uitzen- >

- CCT-bereik van 2700-8000 K en een refresh rate van 600 tot 15k Hz, zeer geschikt voor tv-toepassingen
- Individuele pixelbesturing, waardoor elke RGBW LED afzonderlijk kan worden aangestuurd
- Instelbare PWM-frequentie
- Cirkelvormig prisma- of bloemeneffect

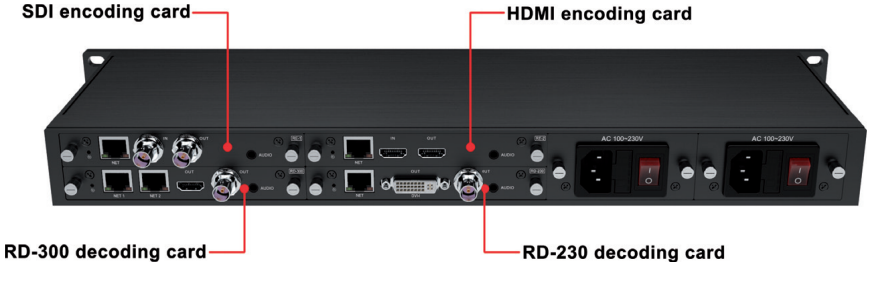
Tel.: +31 (0)45 - 566 77 06 | E-mail: sales@highlite.com | www.highlite.com

infinity

KILOVIEW®

Cradle Series

The reliable and flexible Kiloview Cradle Series include 1RU or 3RU rack-mounted frame and redundant power modules. Combined with 4 channels (1RU), 16 channels / 32 channels (3RU) you are free to mix and insert encoding and decoding card modules for your preferred workflow.



Streaming VALLEY

Distributed by:
Streaming Valley
www.streamingvalley.nl /pro-av

info@streamingvalley.nl
+31 317 210 310

ding in gevaarlijk gebied onbedoeld rechtstreeks tot de reporter en diens locatie te herleiden valt.

Encryptie van content en gegevens ligt voor de hand. Hoe meer moeite het kost om datapakketjes over IP te ontsleutelen des te geringer de kans dat kwaadwillenden daar bij kunnen. Watermerken identificeert de content als echt van de betrouwbare bron afkomstig. Digital Right Management (DRM) beschermt de eigendommen.

Zorg er voor dat alle apparatuur en programmatuur op de juiste wijze geconfigureerd en van de laatste updates voorzien is. Toets wie waar onder welke voorwaarden bij kan komen. Het gevoel van optimale veiligheid moet echt tussen de oren van de medewerkers en gebruikers zitten, anders worden ze laks. Zorg verder voor surveillance op mogelijke fraude via cybercrime. Illegale of vreemde handelingen op systemen en netwerken direct in de kraag vatten.

GANGBARE MAATREGELEN

Hierin verschilt de broadcast-industrie niet veel van het bedrijfsleven. Zorg voor een cybersecurity-cultuur. Alle neuzen dezelfde kant op bij cybersecurity en de bijbehorende gedragsregels. De strategie behoort echt end-to-end te zijn en mag geen losse eindjes kennen. Beveilig de totale supply-keten, die is immers net zo veilig als de zwakste schakel. Houdt deze cybersecurity voor de onderneming up-to-date en voer regelmatig controles uit.

Bescherm je tegen DDoS-aanvallen. Daar is goede software voor. Die onderscheidt goede en slechte verzoeken en schakelt de laatsten uit. Voorkom dat derden via e-mail, netlinks, IOT-apparaten (altijd de veiligheid testen en nieuwste firmware installeren), wearables en (net) nieuw geïnstalleerde applicaties toegang krijgen. Anders staat de ransomware zo op de stoep.

Houd het beleid omtrent wachtwoorden, ID's en logins regelmatig goed tegen het licht. Liefst dubbele of driedubbele verificatie met wachtwoorden, sms, vingerafdruk, gezichts- en netvliesherkenning. En voer (of laat uitvoeren) regelmatig proactief proefhacks uit om te verifiëren dat het allemaal nog echt wel safe is. 24/7/365 monitoring is een must.

Meerdere beveiligingslagen aanbrengen maakt het indringers lastiger en geeft jouw beveiligers meer tijd om tegenmaatregelen te nemen. Pak incidenten zo snel als mogelijk aan (Rapid Incident Respons). En zorg voor effectieve afsluitprotocollen bij het detecteren van cybercrimepogingen. Als laatste: broadcast security is nooit 100% veilig. Zorg voor voldoende backups en verzekering voor als het echt mis mocht gaan. **<**

Een lijst van de meest gangbare maatregelen en bedreigingen vind je bij 35CriticalCyberSecurity Activities_NAB.pdf