Cybercrime en broadcast security

Het is oorlog bij IP

De cyberwar die woedt op IP-netwerken bedreigt ook de broadcast-, entertainment- en evenementenindustrie. Het gaat vooral om het lamleggen en gijzelen, het stelen van content, het vissen naar gegevens van cliënten en disruptie met het ontregelen van de publieke opinie via valse of gestuurde berichtgeving. Reden genoeg om je als omroep, videoproducent en webcaster hiertegen te wapenen.

Tekst Ulco Schuurmans

Op de IBC 2017 was het een van de hoofdthema's: cybercrime vormt een reële bedreiging voor de broadcast- en evenementenindustrie. Het gaat echt niet meer alleen om incidenten van gegapte content, het stelen van wat klantgegevens, een enkel gevalletje van ransomware of een incidentele DNS-aanval. Nee, het betreft momenteel ingrijpende gevaren die het totale wezen van broadcast, streaming (social) media, videoproductie en evenementen kunnen aantasten en ontregelen. Elke 23 seconden is er een serieuze cyberaanval. Een gewaarschuwd broadcaster en evenementorganisator telt voor twee en wellicht zelfs drie! De onachtzame gelegenheid maakt de hackende dief. Kortom, het wordt nu echt tijd om iets te gaan doen aan hackers, cybervandalen, manipulerende vreemde mogendheden en georganiseerde IP-misdaad!

CONNECTIVITEIT IS ALLES

De gehele wereld van communicatie en ICT hangt van connectiviteit aan elkaar. Naar schatting (Cisco) zijn er in

het jaar 2020 zo'n 50 miljard onderling verbonden apparaten. Cybercrime met deze devices en hun verbindende netwerken kan daarom bijzonder lucratief zijn. Behalve de experimenterende eenling en hackergroepen heeft inmiddels ook de georganiseerde misdaad het Internet of Things (IoT) in het vizier. Daar valt veel te halen, zowel financieel als in het verwerven van aanzien. Ook in de cloud kan heel goed de beer los raken. Wie heeft daar wel niet allemaal toegang voor het (mee-)kijken, toevoegen, veranderen en downloaden?

Wellicht nog meer bedenkelijk is dat vreemde mogendheden en groepen met minder frisse ideeën proberen de publieke opinie, verkiezingen en gevoelens van mensen te beïnvloeden. En ook qua commercie weet men van wanten bij misbruik van privacy en klantmanipulatie via Big Data en slinkse broadcast-wegen. De

> "De gehele wereld van communicatie en ICT hangt van connectiviteit aan elkaar. Naar schatting (Cisco) zijn er in het jaar 2020 zo'n 50 miljard onderling verbonden apparaten."

leveranciers van software en hardware houden in de praktijk dikwijls te weinig rekening met cybercriminaliteit. Devices en besturingsprogramma's blijken zo lek als een mandje. Malware wordt regelmatig per ongeluk meegeleverd of gedownload. En via het intelligente broodrooster in de kantine een onbeveiligd IP-netwerk binnen dringen is relatief simpel.

MAKKELIJK?

Er zijn nogal wat succesfactoren bij cybercrime. Het wordt steeds minder moeilijk om het te doen. De benodigde softwaregereedschappen zijn gewoon op Internet (met name op Darknet) te vinden en elke middelbare scholier kan daar zo mee aan de slag. Daarnaast is het eenvoudig op grote schaal toe te passen en daarmee snel flink winstgevend. Er gaan vele tonnen tot miljoenen euro's in om. Ook is het lastig om overal te controleren. Direct toezicht op de eigen IP-broadcast, entertainment- en evenementnetwerken valt vaak nog best te doen. Maar wat als de content en services zich uitbreiden naar YouTube, Facebook, Vimeo, Twitter, Snapchat WhatsApp, Periscope en mojo? Juist ja, dat wordt kijken in een kristallenbol of cybercrime niet ergens op de loer ligt. De pakkans is relatief gering. En een malafide website of server valt door de cybercrime-ondernemer snel te sluiten en elders opnieuw te beginnen. De status die hackers en vreemde mogendheden hiermee kunnen verwerven speelt ook mee. Het juridisch apparaat en strafrecht moeten nog wennen aan cybercrime en de daarbij behorende adequate vervolging met bestraffing. Je komt er als cybercrimineel te vaak gemakkelijk van af.

DNS EN RANSOMWARE

Een van de meest voorkomende vormen van cybercrime vormt het platleggen van complete netwerksystemen. Het bekendste voorbeeld daarvan is de zogenaamde Denial of Service (DoS-)aanval. In geval van een DoSA(ttack) of een distributienetwerk heet dat Distributed Denial of Service (DDoS). De aanbiedende servers en providers worden daarbij met loze verzoeken om service-aandacht zo overbelast dat hun dienstverlening ernstig terugloopt of zelfs geheel uitvalt. Cybercrime maakt daarbij gebruik van grote netwerken (botnets) van computers of andere devices die de servers steeds weer met miljoenen aanvragen bestoken. Dat is uitermate vervelend bij het uitzenden van de sporttopper van het jaar, spannende streaming series of VOD op kabelnetwerken en communicatie met het publiek op evenementen.

Van weer een andere orde is het gijzelen van broadcast- en ICT-systemen. De hackers versleutelen de content- en andere bestanden zodanig dat de gebruikers er niet meer bij kunnen. De zogenaamde ransomware komt stiekem door onachtzaamheid of via een paard van Troje binnen. Dan verschijnen de mededelingen dat jouw systeem op slot staat. Alleen te ontgrendelen door het betalen van losgeld in bitcoins. Gelukkig heeft de nationale politie nu een website over hoe je in een flink aantal gevallen de ransomware toch ongedaan kunt maken: www.politie.nl/themas/ransomware.html.

CONTENT STELEN

Het stelen van content kent meerdere vormen van cybercrime. Gewoon een pro-

GENERAL DATA PROTECTION REGULATION (GDPR) VAN DE EU

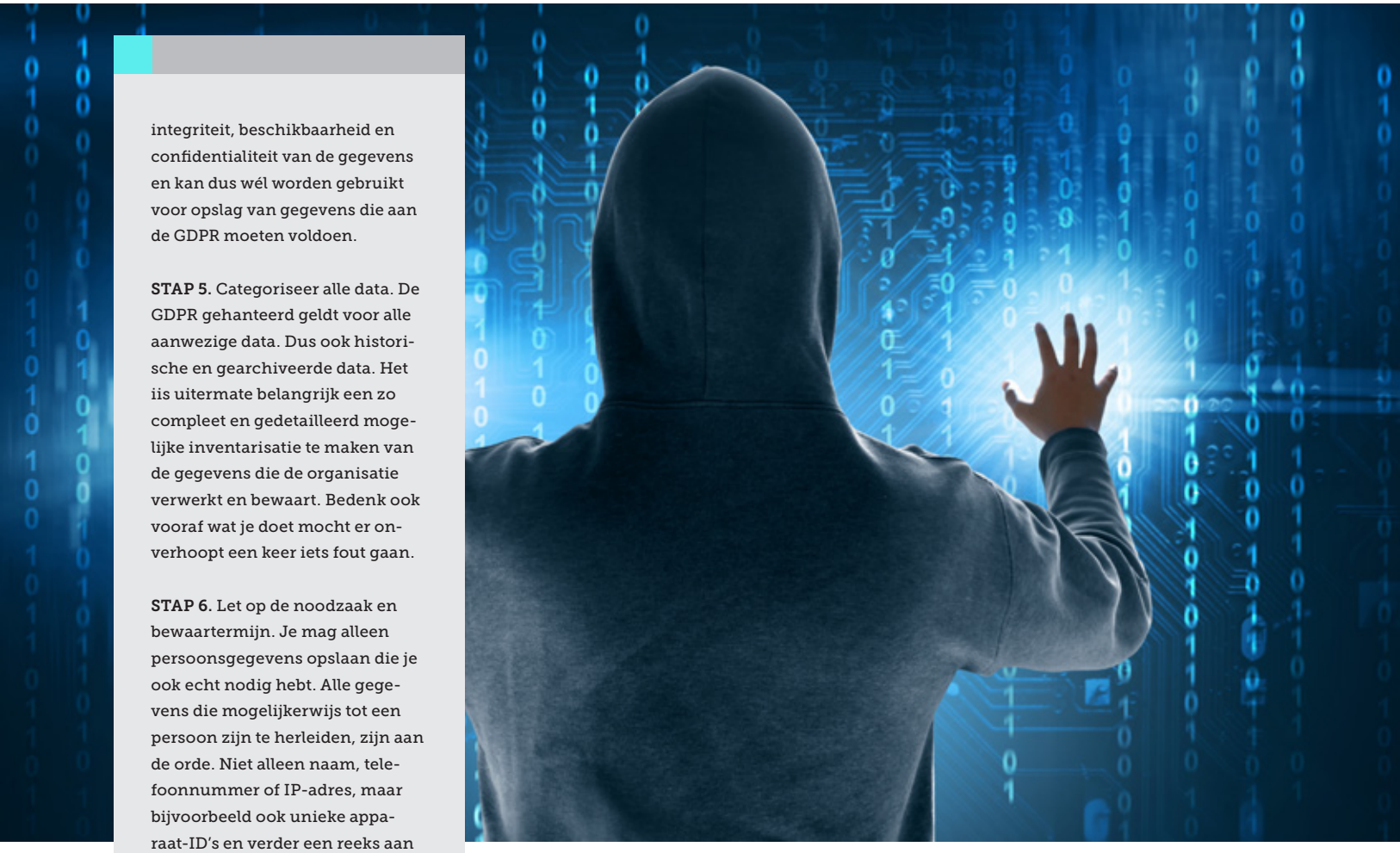
Velen uit de AV- en evenementenindustrie zullen de algemene verordening gegevensbescherming AVG Europees: GDPR voor hun klanten nu niet geheel in het vizier hebben. Harold Koenders, Director Active Archive bij Pronovus attendeerde ons op deze aankomende GDPR regelgeving. Hoe ver zijn we en wat moet er nog gebeuren? Hier een aantal tips en tricks in de vorm van 8 stappen.

STAP 1. Verantwoordelijken. Stel een of meer functionarissen verantwoordelijk als het gaat om ervoor te zorgen dat aan wet- en regelgeving wordt voldaan. Bijvoorbeeld de Chief Information Security Officer.

STAP 2. Het genereren van een overzicht van privacygevoelige gegevens is van fundamenteel belang. Identificeer alle gegevens die volgens de GDPR persoonlijke gegevens zijn. Classificeer deze gegevens aan de hand van de privacy-gevoeligheid. Richt standaard informatiebeveiligingsprocessen in.

STAP 3. Waar bewaart de organisatie de data? GDPR schrijft voor het doel te omschrijven waarom gegevens verzameld zijn. De organisatie mag deze gegevens ook daadwerkelijk alleen voor dit doel gebruiken. Een voorwaarde hiervoor is bovendien dat toestemming is verkregen van degenen over wie je gegevens hebt verzameld.

STAP 4. Controleer de cloud. De publieke Cloud voldoet (nog) niet aan de GDPR omdat het niet toelaat de plaats en confidentialiteit van gegevens te garanderen. Een private Cloud wordt opgezet voor en gebruikt door één organisatie, geeft controle over plaats, >



integriteit, beschikbaarheid en confidentialiteit van de gegevens en kan dus wél worden gebruikt voor opslag van gegevens die aan de GDPR moeten voldoen.

STAP 5. Categoriseer alle data. De GDPR gehanteerd geldt voor alle aanwezige data. Dus ook historische en gearchiveerde data. Het iis uitermate belangrijk een zo compleet en gedetailleerd mogelijke inventarisatie te maken van de gegevens die de organisatie verwerkt en bewaart. Bedenk ook vooraf wat je doet mocht er onverhoopt een keer iets fout gaan.

STAP 6. Let op de noodzaak en bewaartermijn. Je mag alleen persoonsgegevens opslaan die je ook echt nodig hebt. Alle gegevens die mogelijkerwijs tot een persoon zijn te herleiden, zijn aan de orde. Niet alleen naam, telefoonnummer of IP-adres, maar bijvoorbeeld ook unieke apparaat-ID's en verder een reeks aan cookies. Persoonsgegevens die niet meer nodig zijn mag je niet mag bewaren! Klanten hebben richt op inzicht in de verzamelde data en het desgewenst verwijderen daarvan.

STAP 7. En de toegang door derden? Je bent ook verantwoordelijk voor de die je toegankelijk maakt voor derden waarmee je bijvoorbeeld samenwerkt. Het is daarom essentieel dat je alleen de juiste data met de juiste partijen deelt.

STAP 8. Ondersteuning voor eDiscovery (juridisch reviewplatform voor digitale documenten). Voorkom hoge boetes en houdt voor eventueel juridisch onderzoek alles netjes bij. Door het geautomatiseerd vast te leggen is altijd te achterhalen wie ergens wanneer bij kon en wat er allemaal met de data is gebeurd. Daarmee behoort ook eDiscovery tot de mogelijkheden.

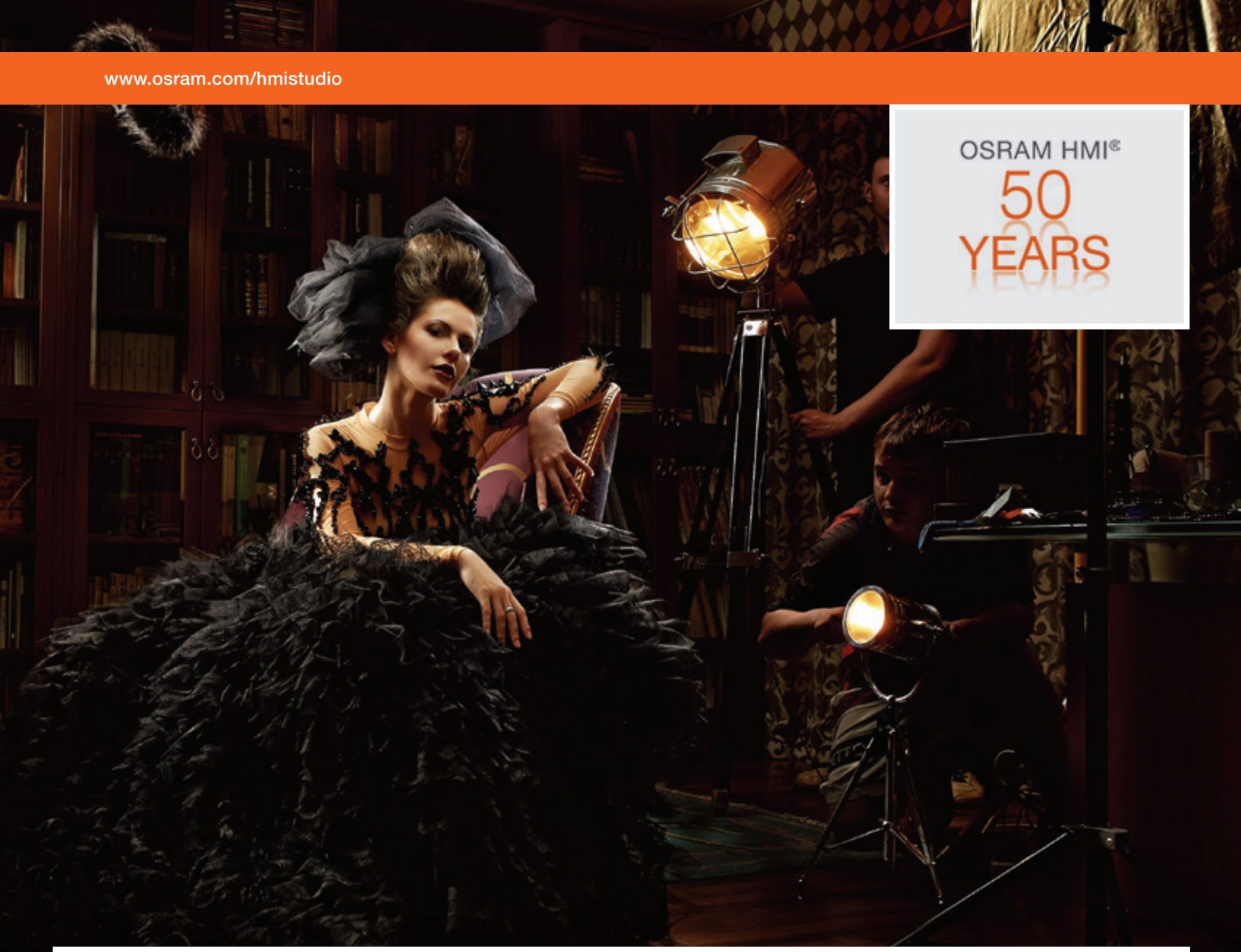
ductie kopiëren of jatten en vervolgens op Internet gratis of te koop aanbieden is al jaren schering en inslag. Dat had tot gevolg een heuse oorlog om het copyright en het vervolgen van malafide distributeurs. In feite verschilt dit allemaal niet zo veel van het vroegere kopiëren van videotapes en DVD's. Alleen gaat het nu nog grootschaliger en gemakkelijker terwijl de daders lastig te achterhalen vallen. Van recentere orde is het gijzelen van nog niet uitgebrachte bioscoopfilms en tv-series. Sony en Netflix kunnen daarover meepraten. Vroeger ging een employee of insluiper er met de filmspoel of videotape vandoor. Tegenwoordig ontvreemdt de hacker het bestand van de studioserver. Even snel een USB-stickie of SD-kaart erin steken, digitale archieftape pikken of lekker online op afstand. Vervolgens dreigt deze cybercrimineel de gestolen producties voortijdig (gratis) online te zetten of gewoon door te verkopen. Daarvoor een afkoopsom betalen blijkt regelmatig zinloos. Na het ontvangen van het geld doen ze het regelmatig alsnog.

VISUAL HACKING

Visual hacking dan. Al vele jaren komt het voor dat bezoekers van bioscopen en evenementen een verborgen videocamera meenemen. Daarmee filmen ze vanuit de zaal de videoproductie of performances op het bezochte evenement. Dat wordt tegenwoordig steeds simpeler: miniatuurcamera's, gemonteerd in kleding of gebruiksvoorwerpen, hoogwaardige smartphones, minipalmtop-videocamera's en smart brillen. De beeldkwaliteit is verrassend goed, maar qua audio blijft het behelpen, tenzij de dader de zaalinstallatie aftapt. Een variant van het content digitaal stelen uit de bioscoop is het brutaalweg aftappen van de e-cinema. Aan de bron, in de zaal of tijdens de transmissie per kabel of satelliet. Een soort visuele content-hacker in the middle.

Een banale vorm van visual hacking is het gewoon over de schouder meekijken. D.w.z. het stiekem meekijken naar de gegevens van andere gebruikers op zijn of haar beeldscherm. Zo valt gemakkelijk aan inloggegevens, wachtwoorden en

www.osram.com/hmistudio



Licht is opvallend

Warm licht voor ‘coole’ scenes met HMI® STUDIO lampen

Een evolutie in licht, de HMI® STUDIO lampenserie maakt haar debuut en levert een moeiteloze prestatie. HMI® STUDIO is een metaal halide lamp met een halogeen kleurtemperatuur van 3.200K voor filmsets, theaterpodia en televisie studio’s. HMI® STUDIO lampen werken in daglichtarmaturen en maken aparte halogeenarmaturen overbodig.

Light is OSRAM

OSRAM

andere bedrijfsinformatie te komen. Het meekijken thuis bij de ontvanger behoort eveneens tot de opties bij visual hacking. Behalve het volgen van toetsaanslagen en browseractiviteiten kan een malwarecookie ook visuele gegevens zoals video en foto doorsluizen.

PTZ- EN CCTV-NETWERKEN AT RISK

Een categorie apart zijn de onbeschermde CCTV-netwerken. Het begint al simpel bij de beveiligingscamera in en om het huis of bedrijf. Als de gebruiker deze via Internet kan bekijken lukt een cybercrimineel dat ook. Daarmee liggen de privacy en bedrijfsgeheimen zo op straat. Investeer in beveiligde PTZ-camera's en encryptie! Panasonic voorziet in veilige CCTV-netwerken met beschermde veilige videosurveillance. Het bedrijf spreekt zelf van Secure Communication op PC-niveau voor IP-camera's. Je bent hiermee beschermd tegen spoofing (valse data invoegen), video tampering (knoeien met het beeld), altering (beelden veranderen) en snooping (het stelen van inloggegevens en wachtwoorden). Dat verloopt zowel via dataversleuteling (encryption), communicatie-encryptie en verificatie met keys.

Een schaal groter is het PTZ-netwerk voor video-opnamen bij sport, evenementen en tegenwoordig ook filmproductie. Die gaat over IP-netwerken en NDI. Wie kunnen daar dan wel niet op meekijken, inbreken en content stelen?

> "Niets is te dol voor de vernielkick."

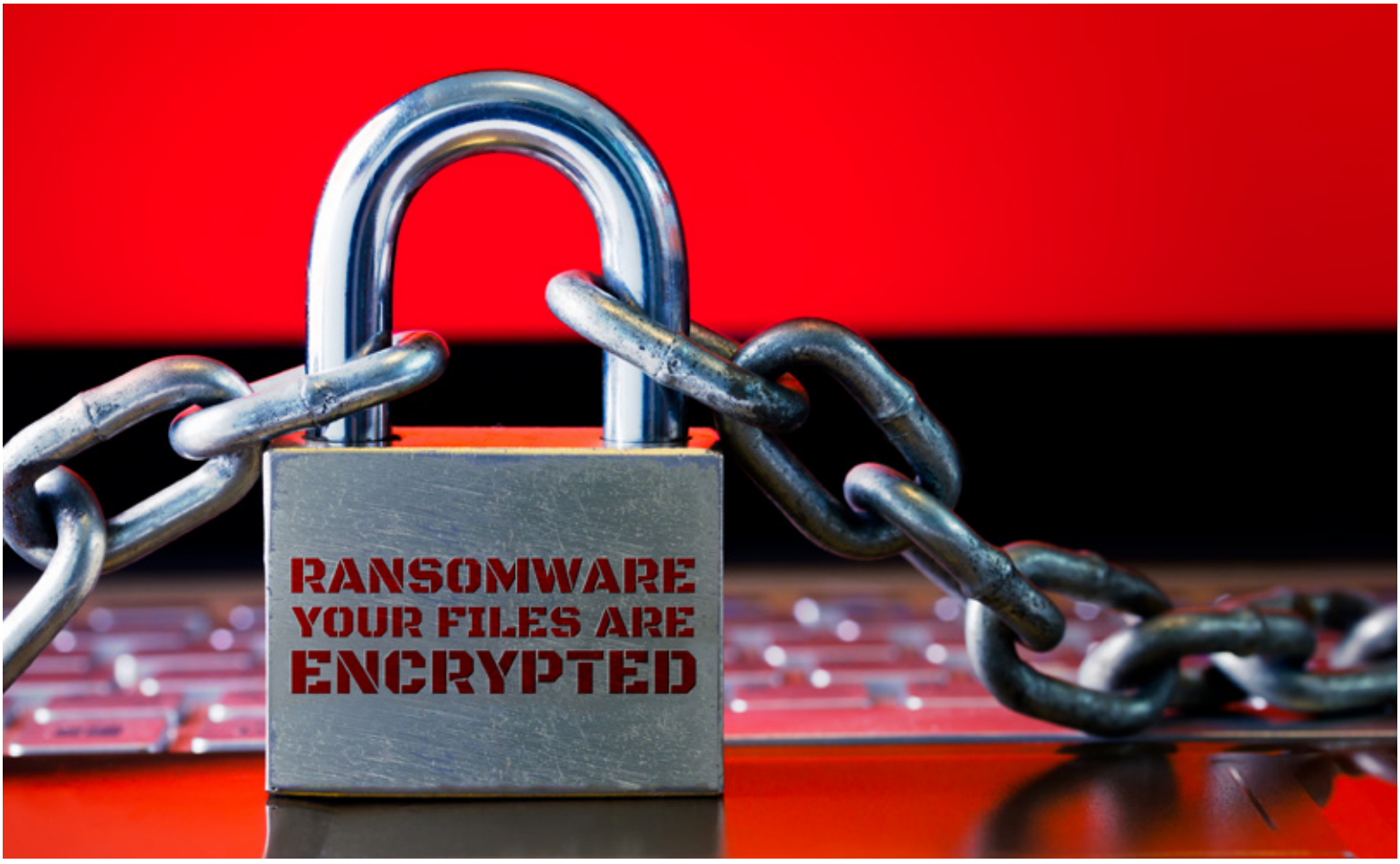
Video leaking behoort zeker tot de criminele mogelijkheden. Het aftappen van draadloze verbindingen bij voetbalstadions kwam al ruim vijftien jaar geleden voor. Nu kan de ondernemende hacker complete sportwedstrijden en optredens bij evenementen rechtstreeks van het netwerk aftappen en global streamen. Bij betalende kijkers uiteraard niet gewenst!

IP-HOOLIGANS

Het doelbewust saboteren en vandaliseren is een tak van cybercrime met meerdere wortels. Bekend zijn het beeld vervormen, het geluid verzieken, het scherm op zwart, rare beelden of teksten toevoegen en het niet meer kunnen tunen of zappen. Het kan gaan om actiegroepen die een uitzending of evenement willen verpesten. Of gewoon om criminele afpersing, een bekend handelsmerk van de onderwereld en maffia. Daarnaast ook de gewone criminele vandalen, de IP-hooligans zullen we hen maar noemen. Niets is te dol voor de vernielkick. En daarnaast heb je nog 'gewoon' accidentele baldadigheid door jongeren.

VISSEN BIJ DE KIJKER

Als provider van videoproducties mogen de kijkers thuis en bezoekers van evenementen toch wel enige veiligheid en bewaking van de privacy van u verwachten. Regelmatig zijn er meldingen van diefstallen omtrent cliënt- en betalingsgegevens bij grote bedrijven. Pay-tv en VOD zijn een interessant doelwit voor de hierin geïnteresseerde



cybercriminelen. Een stap verder gaat het via jouw IP-verbindingen bij de kijker thuis meekijken. Dat kan dan weer leiden tot fishing naar diens bank-, bedrijfsgevoelige en privacygegevens. Een variant vormt het in kaart brengen van het kijkersgedrag. Dat is veel geld waard voor het aanbieden van reclame, emotional targetting en het in diskrediet brengen van personen. Bij een hack bij Sony in 2014 werden tevens gegevens van werknemers en sterren gestolen. Schade inclusief een aantal films op piratesites bedroeg ruim €15.000.000,-.

DISRUPTION

Een relatief nieuw en reëel IP-gevaar is de doelbewuste disruptie van audiovisuele beeldvorming door cybercriminelen. Daar zijn inmiddels al tal van voorbeelden van. Het beïnvloeden van verkiezingen bijvoorbeeld, het in kwaad daglicht stellen van bepaalde personen of groepen in de maatschappij, gestuurde beeldvorming om (politieke) beslissingen er door te krijgen en het creëren van angst en dreiging.

Video is een medium dat heel belevend aanspreekt. Een verkeerde setting is zo geschapen of een gevoelige snaar snel beroerd. Vreemde mogendheden, niet zo frisse actiegroepen en fantasten die willen opvallen spinnen daar goed garen bij. Gewone leveranciers van valse of lasterende berichten, de videotrollen, zijn tot daar aan toe. Er is echter ook een aparte specialistische industrie ontwikkeld voor het beïnvloeden van de publieke opinie en het ontwrichten van berichtgeving.

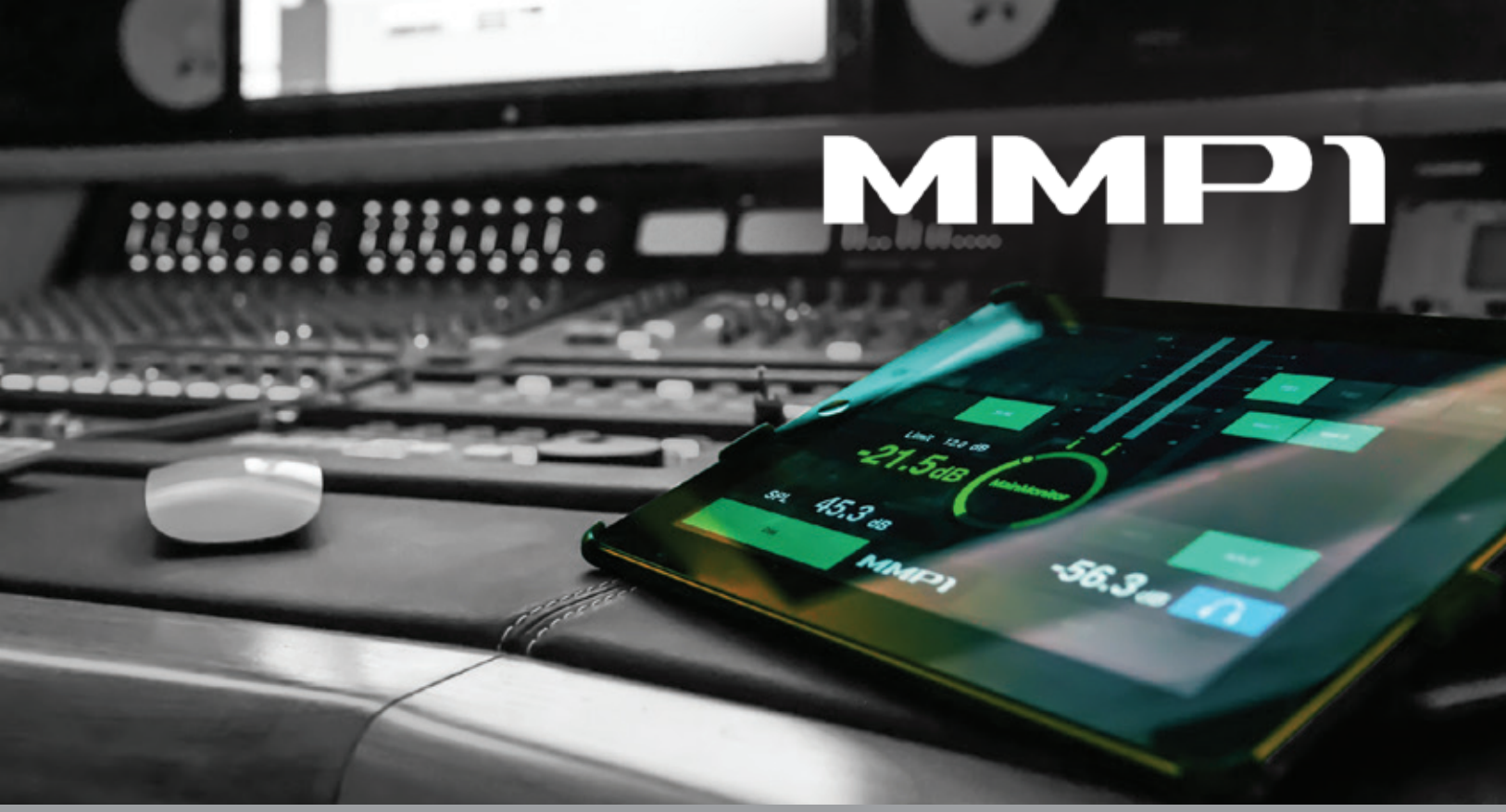
> "Een relatief nieuw en reëel IP-gevaar is de doelbewuste disruptie van audiovisuele beeldvorming door cybercriminelen."

Kijk dan straks ook niet verbaasd op als deze vorm van cybercrime uw uitzendingen of beeldschermen op evenementen tracht te infiltreren. Net echte valse nieuwsuitzendingen, suspecte emoties bespelende commercials en wellicht straks ook een beruchte machthebber uit Azië die ineens het publiek op een Nederlands evenement via de big screens toespreekt.

Enkele treffende voorbeelden zijn er al. In 1938 leidde in de VS een realistisch hoorspel over de mars-invasie uit War of the Worlds van H.G. Wells (Gebracht door Orson Wells in het Mercury Theatre on Air) tot een ware massahysterie. In Minnesota gebeurde hetzelfde met een realistische uitzending over een uitbraak met zombies op het lokale tv-station.

DNS ENCRYPTION

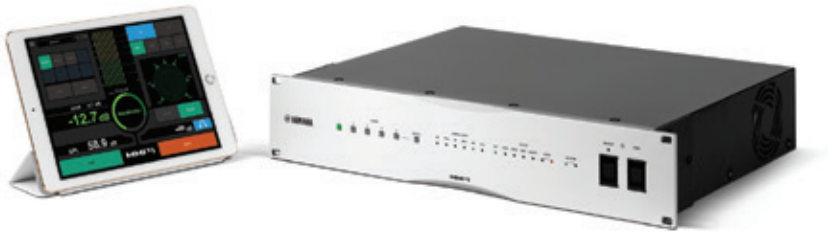
Een belangrijk stukje klantenbescherming is de zogenaamde DNS-encryption. Het aan de Domein Name System verbonden Internetverkeer kan het gedrag van uw klanten op IP-netwerken nauwkeurig in kaart brengen. Daarbij is het uiteraard niet de bedoeling dat derden met deze privacygevoelige gegevens aan de haal gaan. Zowel veiligheidsdiensten als cybercriminelen zullen daar op azen. Het versleutelen van deze data, DNS encryption, voorkomt ongewenste inzage afdoende.



Big studio monitor management for **in the box** productions

The new Yamaha MMP1 Studio Monitor Management System

Versatile, great-sounding and refreshingly affordable, the new Yamaha MMP1 brings sophisticated monitor management to DAW-based production environments. From stereo through to complex, multi-channel formats like Dolby Atmos, MMP1 delivers flexible routing of all essential audio throughout the studio, along with the powerful bass management control, time alignment delays and six-band room EQ necessary to optimise your monitoring for your production space. MMP1 is easy to configure and operate via Mac/Windows Apps, and there's also an iPad App for convenient control of all essential parameters.



The MMP1 Studio Monitor Management System: Part of Yamaha's continuing commitment to enhancing the audio production process

- Comprehensive Monitor Control
- Outstanding Speaker Management Precision
- Flexible Bass Management
- Full-Feature Channel Processing
- Post-Production Recording Support

For more information please visit **www.yamahaproaudio.com**

YAMAHA commercial audio

Inspired sound

WAT TE DOEN?

De keten is bij cybersecurity net zo sterk als de zwakste schakel. Gelukkig doen relatief eenvoudige beschermingsmaatregelen al behoorlijk veel. De aanpak van cybercrime betreft doorgaans drie verschillende fasen:

Als eerste de preventieve netwerkhygiene. Voorkomen is dikwijls al meer dan het halve werk. Het gaat daarbij vooral om een Firewall installeren, de juiste beschermings- antivirussoftware draaien, regelmatige back-ups van de systemen maken, het bijhouden van updates voor de IP-netwerken en aangesloten apparatuur (ook camera's, smartphones, routers, switchers, tablets e.d.), veilige IP-protocollen en encryptie.

Daarnaast veilige gedragsregels voor het personeel opstellen. Laat hen bij voorkeur dubbele inlogbeveiliging (naast de inloggegevens en wachtwoord ook een smscode, vingerafdruk of irisscan) gebruiken en voorkomen dat er datadragers rondslingeren. Verder veilige browsers gebruiken, geen mails, sms-jes en bestanden van onbekende herkomst openen en niemand over de schouder laten meekijken

Maak de werknemers en klanten bewust van het gevaar van cybercrime via IP.

Laksheid en onzorgvuldigheid vormen een belangrijke oorzaak voor binnendringende hackers. Vergeet daarbij de klanten en partners niet. Wijs fabrikanten van slimme apparaten zoals tv's, smartphones en IP-camera's op de kwetsbaarheid voor cybercrime. De smart tv en smartphone zijn bekende lekken.

Ten tweede: call in the experts. Een expert het systeem laten doorlichten op kwetsbaarheid (analyse van) en afdoende beveiliging is feitelijk een must. Het kost geld, maar kan later veel ellende en hoge kosten voorkomen. Bovendien kan de expert direct ingrijpen bij een aanval van cybercriminelen of –vandalen.

Ten derde, als het dan toch gebeurt: gewoon stom is het maar verzwijgen en betalen of helemaal niets doen. Daar spinnen de cybercriminelen garen bij! Ze gaan gewoon ongestraft door en kunnen weer anderen in de industrie benadelen.

Twee te ondernemen acties: 1. Aangeven bij politie/justitie, desnoods anoniem. 2. Naast het strafrechtelijk ook civielrechtelijk aanpakken. Trek de criminelen het financiële vel over de oren. Dat schrikt flink af.

EXPERTWERK

Als de tegenstanders over experts beschikken dan zullen de broadcasters en organisatoren van evenementen dat voor cybercrime ook moeten doen. Goed geïnvesteerd geld en vaak goedkoper en verrassend effectiever dan verwacht. Er komen steeds meer ook voor de AV-industrie deskundige beveiligingsbedrijven en bonafide hackers tegen cybercrime. O.a. Deloitte en Touche, Capgemini, Zerocopter, Compumatica , CGI, Panasonic, Samsung Evolve (Mobiel), ON2IT, Pine, Korton, Nixu, ACA IT, KPN, Sophos en Ziggo. Vanuit de Nederlandse overheid is er het Nationale Cyber Security Centrum. Er zijn ook enkele in de gevolgen van cybercrime en diefstal van content (intellectueel eigendom) gespecialiseerde advocatenkantoren, zoals Dirk Zwager. Daarmee pak je de cybercriminelen in hun eigen beurs.

> "AI (artificial intelligence) herkent uiterst nauwkeurig patronen, schat onverwachte acties en gebeurtenissen in, leert snel en houdt alle bekende gegevens over de lopende cyberwar bij."

AI-BESCHERMING

Nog heel nieuw en deels in ontwikkeling is de kunstmatig intelligente cybersecurity. AI (artificial intelligence) herkent uiterst nauwkeurig patronen, schat onverwachte acties en gebeurtenissen in, leert snel en houdt alle bekende gegevens over de lopende cyberwar bij.

Langzaam maar zeker raakt de AV- en evenementenindustrie doordrongen van de gevaren bij cybercrime. En bij wie daarvan al het slachtoffer werd zit de schrik er vaak goed in. Zoals gezegd valt er gelukkig relatief veel aan te doen en is het zelfs onze plicht om de kijkers en klanten hier tegen te beschermen.