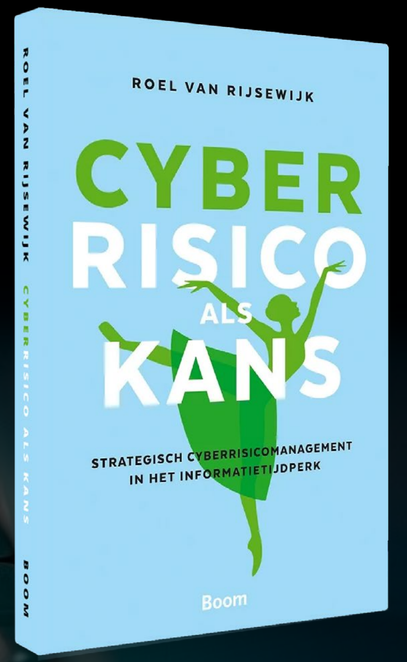
OnlineSecurity Game.com

10 Tips van Roel van Rijsewijk

Director Cyber Defense Thales en schrijver van het baanbrekende boek “Cyberrisico als kans”.



Games 4Growth.com Serious Game Publishers

De Online Security Game is een dienst van Games.4Growth, uitgever en implementatiepartner voor serious gaming.

OnlineSecurity Game.com

Voorwoord

“Het is niet de vraag óf je wordt aangevallen als organisatie, maar wannéér je wordt aangevallen door cybercriminelen.”

Welke keuzes je ook maakt, IT beveiligingsmaatregelen beschermen je nooit 100%. Ook het bewustmaken (awareness) van je medewerkers is niet afdoende. Je medewerkers zijn tenslotte je eerste defensielijn. Ook al weten ze alles over phishing, de cyberrisico’s en malware, dat betekent nog niet dat ze waakzaam en weerbaar zijn. ‘Weten’ is niet de uitdaging. ‘Doen’ is waar het om gaat.

Hoe krijg je bewuste, waakzame en weerbare medewerkers? Hoe maak je van ‘je zwakste schakel’ je ‘first line of defence’?

Door het toepassen van deze 10 tips en inzichten zet je de eerste stap.

Veel leesplezier,

Roel van Rijsewijk

OnlineSecurity Game.com

1 Gedragsverandering is het doel, bewustwording niet.

Vaak hoor ik ‘de medewerkers zijn de zwakste schakel’ als we het hebben over de Online Security strategie. ‘Ze weten niet welk gevaar er buiten is! Als we ze nu maar bewust maken van het gevaar en de risico’s, dan creëren we meer veiligheid.’

Niets is minder waar! De meeste medewerkers snappen best wat de digitale online gevaren en bedreigingen zijn. Maar het zijn en blijven mensen. En mensen zoeken altijd de makkelijkste weg. Als jouw instructie het werken voor je medewerkers lastiger maakt, dan kan ik je beloven dat ze zich er niet aan gaan houden. Verdiep je in ‘hoe’ de medewerkers de IT omgeving gebruiken. Kijk waar ze risico’s nemen en waarom. Kijk hoe jij het werken makkelijker voor ze kan maken. Dan pas gaan mensen ander gedrag vertonen.

Tip: Gedragsverandering is wat je zoekt. Geen awareness!

OnlineSecurity Game.com

2 Ken je vijand! Om de vijand te bestrijden, moet je die begrijpen.

Wie zijn je vijanden als het gaat om Online Security? Waar komt je bedreiging vandaan? Wat is het meest waardevolle wat ze kunnen stelen, blokkeren of beïnvloeden?

Leef je in. In de hackers van deze wereld. Snap waarom ze het doen. Waarom ze het bij jullie zouden doen! Ken het verschil tussen de drijfveren van een White, Grey en Black hat hacker. Wat is interessant bij jullie? Waar zit de grootste waarde voor een hacker? En ga dan gericht aan het werk om die kwetsbare, interessante, en waardevolle plekken te beschermen.

OnlineSecurity Game.com

3 Zorg voor goed overzicht van je IT landschap. Dat is belangrijker dan alle beveiligingssystemen.

Wees waakzaam. Overzicht is een eerste vereiste in het steeds verder groeiende IT landschap.

Grote organisaties hebben een bijna onoplosbaar probleem. De grote financiële instellingen weten bijvoorbeeld niet eens wat voor IT zij hebben. Eigenlijk zouden zij alle troep moeten weggooien en opnieuw moeten beginnen. Mkb'ers hebben geen geld om een speciaal veiligheidscentrum in te richten, maar ze zijn klein genoeg om te kunnen monitoren of er iets vreemds gebeurt. Die hoeven niet de monitoring service van Symantec te kopen. Dat is voor hen ook veel te duur. Maar ze moeten wel waakzaam zijn.

Tip: Creëer overzicht en wees waakzaam.

OnlineSecurity Game.com

4 Wees als een ballerina in plaats van als een ridder.

Als je de organisatie een harnas aantrekt, klinkt dat heel veilig. Maar je kunt je niet snel omdraaien met een harnas aan en als je van het paard afvalt, lig je weerloos op de grond.

Een ballerina is kwetsbaar, maar ook heel wendbaar en sterk. Innovatie, IT, Online Security en hackers in deze wereld zijn wendbaar en flexibel. Bewegelijk en snel. Ze zijn niet statisch. De hele organisatie als een fort barricaderen geeft een schijnzekerheid.

OnlineSecurity Game.com

5 Durf bij cyberrisico’s kwetsbaar te zijn. Het gaat een keer mis, daar kan je op rekenen. Leer daar van. Kwetsbaarheid is een kracht.

Alle organisaties zijn het doelwit van hackers en je kunt je nooit 100% beveiligen tegen cyberrisico’s. Als je wilt meegaan met de technologische ontwikkelingen moet je accepteren dat het fout gaat. Maar wees wel weerbaar. En leer daar van! Gebruik elke indringer als lering ter verbetering.

Vergelijk het met het menselijk lichaam. Als je thuis blijft zitten, zal jou zeker niets gebeuren. Maar als je contact wilt hebben met andere mensen is er het risico dat je ziek wordt. Daar heeft je lichaam een immuunsysteem voor ontwikkeld. Speciaal omdat het lichaam weet dat een mens contacten nodig heeft, maar wel met een goede weerstand. Zo weet je als organisatie ook dat je je niet 100% kunt afsluiten van de buitenwereld.

Tip: Zorg daarom voor een goede weerstand.

OnlineSecurity Game.com

6 Wordt risico zoekend in plaats van risicomijdend.

Het is van belang dat de verantwoordelijken voor de Online Security, bijvoorbeeld de Security Officer, wat meer risico zoekend wordt, in plaats van risicomijdend.

Te grote focus op voorkomen van aanvallen stopt het innovatievermogen. Risico's zijn een gevolg van innovatie. Je loopt altijd achter de feiten aan en kan nooit 100% veiligheid garanderen. Zoek de risico's zelf op, anders vindt een ander ze voordat jij ze vindt. En zorg er dan voor dat je een goed ontdek- en alarmeersysteem hebt.

OnlineSecurity Game.com

7 Richt je op ‘verdediging’ (defense, detectie en respons), minder op ‘beveiliging/veiligheid’ (security).

Het is een illusie om je online veiligheid 100% te garanderen. Het doel moet zijn dat je de risico’s reduceert tot een acceptabel niveau.

Een bedrijfsnetwerk moet bijvoorbeeld goed bereikbaar zijn. Het idee dat dat ook betekent dat hackers erbij kunnen, jaagt veel mensen schrik aan. Maar zelfs een netwerk dat vanaf het internet volledig onbereikbaar is, kan nog steeds worden gekraakt.

Richt je op de verdediging

Security suggereert een zekerheid die niet werkelijk bestaat. Je bent nooit 100% secure. Waar een organisatie wél voor kan zorgen is dat de verdediging zo goed op orde is dat de risico’s aanvaardbaar worden en de angst voor security-incidenten wordt weggenomen.

Een goede defensie geeft je organisatie de vrijheid, de rust en het vertrouwen om te ondernemen en te innoveren.

Welke scenario’s heb je als je een inbraak hebt ontdekt? Kent iedereen het protocol? Voelen je mensen zich vrij en veilig om hun eigen ‘fouten’ proactief te melden? Krijgen ze dan een straf of neem je ze mee in het minimaliseren van de effecten van hun ‘fout’? Leren ze iets van hun ‘fout’ en kunnen ze daarna wellicht andere collega’s waarschuwen? Richt je ‘Repons’ actie in.

OnlineSecurity Game.com

8 Breng je Olifantenpaadjes in kaart en snap waarom die er zijn.

Wat we zien is dat mensen wel degelijk weten wat de risico's zijn, maar er niet naar handelen. Waarom is dat zo?

Angst is een hele slechte raadgever. Wat we nu nog vaak zien is dat maatregelen voor cybersecurity gedreven worden door de angst voor aansprakelijkheid en onrealistische verwachtingen. Je kunt zoveel Security Awareness programma's draaien als je wilt, maar het risico wordt nooit nul. Wat je wél kunt doen is zorgen dat risico's acceptabel worden.

Een restrictief security-beleid zorgt uiteindelijk altijd voor olifantenpaadjes. Een omgeving 100% dichtzetten is naast onmogelijk, ook gewoon onwenselijk. Het zorgt alleen maar voor meer frictie en ongewenst eigen initiatief van medewerkers.

Single sign-on (SSO)

Olifantenpaadjes zijn short cuts die het werken voor medewerkers makkelijker maken. Denk hierbij aan het opschrijven van wachtwoorden, het plakken van wachtwoorden op de pc, etc. Een nachtmerrie voor elke CISO, maar waarom doen je medewerkers dat? En op welke manier kan jij het voor hen makkelijker maken. Een single sign-on is een voorbeeld van een vergemakkelijking, die gelijktijdig de veiligheid op niveau houdt.

OnlineSecurity Game.com

9 Stap van de compliance gedreven focus af.

Vaak zie ik dat het zetten van ‘vinkjes’, door compliance gedreven, het doel wordt. ‘We hebben aan alle vereisten voldaan. Alle vinkjes zijn gezet. We zitten goed’.

Dat is niets anders dan een schijnzekerheid. Als je eerlijk kijkt weet je dat audits, checklist en vinkjes altijd achter lopen op de actualiteit. Het gaat om beveiligingen tegen bedreigingen die in het verleden plaatsvonden. Niets over innovatie en de toekomst.

In de meeste sectoren zijn er allerlei beveiligingsrisico’s bij nieuwe apparatuur en instrumenten. Organisaties willen de verantwoordelijkheid daarvoor zoveel mogelijk leggen bij de producenten en leveranciers. De producten moeten voldoen aan lange waslijsten van beveiligingseisen.

Compliance gedreven aanpak

Het gevolg is dat die producenten en leveranciers op hun beurt contractueel willen vastleggen waar hun verantwoordelijkheid eindigt en die van de organisatie begint. Dit leidt tot een compliance gedreven aanpak. Waarbij cyberrisico’s een bedreiging zijn en innovatie wordt afgeremd. Cyberrisico’s worden hierbij alleen gezien als iets dat geld kost en eigenlijk niets oplevert.

OnlineSecurity Game.com

10 Creëer een Red Team

Ga de uitdaging aan en laat je IT omgeving bewust aanvallen. Zoek naar de zwakke plekken in je systeem.

Op basis van die aanvallen en de evaluatie van de aanval kijk je naar de zwakke plekken. Die ga je verstevigen. Je minimaliseert risico's, stimuleert innovatief denken en doen en zorgt voor een flexibele weerbaarheid.

Red Team

Een Red Team bestaat meestal uit White (Social) Hackers, soms aangevuld met eigen medewerkers die de uitdaging ook willen aangaan om jouw beveiliging te testen.

Tip: Maak een gewoonte van het testen en deel de ervaringen.

OnlineSecurity Game.com

Wil je meer weten over de visie van Roel van Rijsewijk en over de mogelijkheden die je zelf hebt om je collega's en medewerkers weerbaarder te maken? En hoe je van jouw medewerkers een sterke 'first line of defence' maakt?

In samenwerking met Roel van Rijsewijk heeft Games.4Growth een gegamificeerd online security programma gebouwd. Met de Online Security Game zorgen we ervoor dat jouw medewerkers binnen drie weken op een speelse en actieve manier getraind worden en die verdedigingslinie écht actief wordt.

Maak binnen drie weken van jouw werknemers een eerste verdedigingslinie met de onlinesecuritygame.nl

Mensen maken het verschil. Ook in digitale veiligheid.

Ja, ik wil een inspirerende demo

OnlineSecurity Game.com

+31 (0)85 06 02 888
onlinesecuritygame.com
OnlineSecurityGame@4growth.com

Games 4Growth.com Serious Game Publishers

De Online Security Game is een dienst van Games.4Growth, uitgever en implementatiepartner voor serious gaming.