

11:11 Systems deelt tips voor het gebruik van regelgeving om de cyberweerbaarheid te versterken

LONDON, UK, June 12, 2024

/EINPresswire.com/ -- Geschreven door Sean Tilley, Senior Director Sales bij 11:11 Systems

In het moderne, onderling verbonden wereldwijde landschap staat operationele en cyberveerkracht hoog op de lijst van bedrijfsprioriteiten. Het digitale tijdperk brengt tal van ongekende kansen met zich mee voor innovatie en groei, maar staat ook in het teken van nieuwe cyberdreigingen.

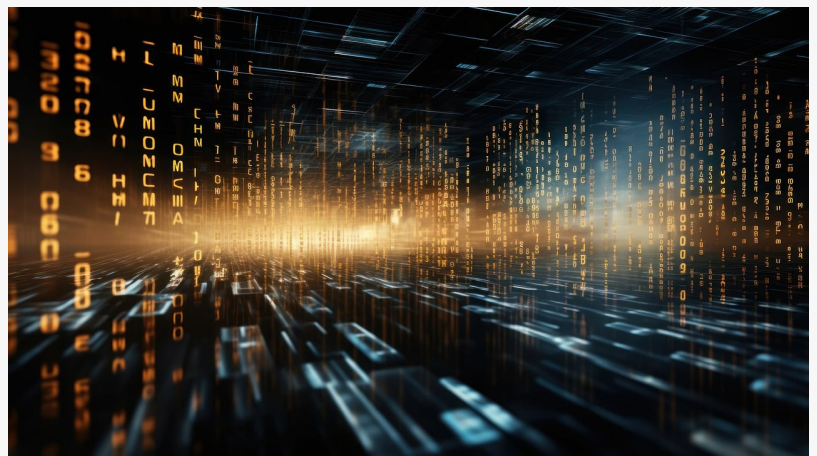
Er zijn veel vormen van bedreigingen, van aanvallen van ransomware en gedistribueerde denial-of-service (DDoS) tot phishing en sociale engineering. Uit de regelmaat van de krantenkoppen over schokkende aanvallen wordt het duidelijk dat dergelijke bedreigingen, de daaruit voortkomende gegevensinbreuk en downtime cruciale gevolgen hebben voor bedrijven, het vertrouwen van het publiek aantasten en aanzienlijke economische verliezen opleveren.

Deze bedreigingen worden versterkt door de explosieve groei in werken en toegang op afstand. Dit alles heeft kwetsbaarheden aan het licht gebracht in wat voorheen werd beschouwd als een robuuste digitale weerbaarheid. Cybercriminelen zijn meer gedurfd en innovatief. Ze grijpen hun kans met deze nieuwe kwetsbaarheden om meer wijdverbreide, geavanceerde en schadelijke aanvallen dan ooit uit te voeren.

In dit opkomende landschap van bedreigingen heeft de focus zich verplaatst naar naleving van de wet- en regelgeving en operationele en cyberveerkracht om risico's tot het minimum te beperken en te zorgen dat bedrijven een aanval overleven.

Regelgeving stuurt cyberveerkracht aan

Cyberveerkracht is een strategische en allesomvattende benadering. Bedrijven verbeteren hiermee hun mogelijkheid om cyberaanvallen en -incidenten te voorzien, te voorkomen, erop te



reageren en zich te herstellen.

Overheden en regelgevende instanties wereldwijd hopen werkelijke operationele en cyberveerkracht te bereiken middels regelgevingskaders die technologie, mensen, processen en informatie omvatten. Om deze complexe regelgevende omgeving na te leven is een strategische aanpak vereist. Begrip van de fijne nuances van elke wet, de gevolgen hiervan en de tijdlijnen voor naleving zijn cruciaal.

Regelgeving zoals de AVG, HIPAA en Sarbanes-Oxley (SOX) hebben vorm gegeven aan de manier waarop bedrijven hun gegevens beschermen. Nieuwe op stapel staande mandaten zoals NIS2, DORA, en FCA CP19/32 gaan nog een stap verder: ze geven een hele nieuwe vorm aan hoe bedrijven gegevensbeveiliging, -privacy en cyberveiligheid moeten aanpakken om te zorgen dat ze hun klanten dezelfde hoge servicesniveaus blijven bieden, ondanks de explosieve groei aan bedreigingen.

Naleving van wet- en regelgeving is niet alleen een wettelijke verplichting, het is een strategische noodzaak voor operationele veerkracht en hiervoor is een allesomvattende, goed geplande aanpak van cyberveiligheid noodzakelijk. Bedrijven kunnen voordeel halen uit een herbeoordeling, versterking en vernieuwing van hun houding ten opzichte van cyberveiligheid. Zo wordt de naleving van wet- en regelgeving een concurrentievoordeel.

De kosten van onveiligheid in cyberspace

In 2023 stegen de totale kosten van gegevensinbreuk tot USD 4,45 miljoen, het hoogste bedrag in het 19-jarig bestaan van het rapport [Cost of Data Breach](#) van het Ponemon Institute en IBM. Er wordt geen stabilisatie verwacht van deze opwaardse trend, de experts waarschuwen voor een blijvende toename van zowel de regelmaat als de geavanceerdheid van cyberaanvallen.

E-mail, de meestgebruikte tool voor bedrijfscommunicatie, heeft zich neergezet als een van de meest significante kwetsbaarheden en is verantwoordelijk voor ongeveer [94% van alle huidige malware](#). Phishing, een methode die gebruikmaakt van menselijke fouten en gebrek aan kennis van cyberveiligheid, blijft de meest voorkomende vorm van cybercriminaliteit.

Van financiële verliezen, klantverloop en schade aan de reputatie tot langdurige herstelprocessen en juridische gevolgen, cybercriminaliteit heeft ingrijpende gevolgen en treft bedrijven in elke branche en van elke grootte. Volgens [Cybersecurity Ventures](#) zal cybercriminaliteit USD 9,5 biljoen aan schade veroorzaken in 2024 en USD 10,5 biljoen in 2025. Minder dan 10 jaar geleden was dit nog USD 3 biljoen. Als cybercriminaliteit een land was, was dit de op twee na grootste economie na de VS en China.

De toename in cyberincidenten en de bijbehorende kosten sturen nieuwe regelgevingen aan in cyberveiligheid en gegevensbescherming.

Verschuiving van reactieve naar proactieve cyberstrategieën

In de hele wereld zien overheden en regelgevende instanties de dringende noodzaak in dat digitale infrastructuren moeten worden versterkt tegen de opkomende cyberdreigingen en de aansprakelijkheid als gevolg van defecte of kwaadaardige AI-producten (artificial intelligence). Het doel is om niet alleen reactief te reageren, maar om een proactief, veerkrachtig kader te bepalen dat cyberdreigingen en verstoringen voorziet en de benodigde weerstand biedt.

Nieuwe regelgeving heeft echter diepgaande gevolgen voor bedrijven. Er is een verschuiving nodig van traditionele methoden voor cyberveiligheid naar meer geïntegreerde, allesomvattende strategieën die niet alleen technische oplossingen omvatten, maar die zich ook richten op bedrijfscultuur, grondige planning en bewustzijn van alle medewerkers op elk niveau.

Met de toename van cyberdreigingen is cyberveiligheid het belangrijkste onderwerp van gesprek in elke directiekamer. Bedrijven moeten up-to-date en flexibel zijn om nieuwe regelgeving na te leven en hun digitale middelen en toekomst veilig te stellen. De kloof tussen bewustzijn en gereedheid onderstreept de noodzaak voor een strategische herziening in hoe bedrijven cyberveiligheid en cyberveerkracht aanpakken.

Regelgeving en cyberveerkracht

Voor bedrijven betekent de ontwikkeling van regelgeving dat cyberveiligheid en gegevensbescherming niet langer meer IT-kwesties zijn, maar integraal onderdeel uitmaken van bedrijfsbestuur en strategie. Bedrijven hebben een allesomvattende aanpak nodig om zich aan deze regelgeving aan te passen. Juridische naleving moet worden gecombineerd met robuuste methoden voor cyberveiligheid en gegevensherstel, personeelstraining en controle van systemen om een veerkrachtig operationeel kader te ontwikkelen dat de uitdagingen van een gedigitaliseerde economie het hoofd kan bieden.

Destiny Gillbee
C8 Consulting Ltd.
11-11systems@c8consulting.co.uk

This press release can be viewed online at: <https://www.einpresswire.com/article/719104675>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.