socured
TAKING CARE

In 6 stappen naar een betere databescherming

In 6 stappen naar een betere databescherming

Een goed programma voor databescherming en -beveiliging vereist meer dan het implementeren van bepaalde technologieën. Door naast technologie rekening te houden met mensen, processen en communicatie kun je een strategie creëren die met je bedrijf en de wereld kan meegroeien.

1. STEL EEN TEAM SAMEN DAT VERANTWOORDELIJK IS VOOR DATABESCHERMING

Als het gaat om databescherming, is samenwerking essentieel. In alle delen van de organisatie moeten mensen samenwerken om een holistische strategie voor het beschermen van organisatiedata te ontwikkelen, vooral in het tijdperk van hybride werken. Creëer afstemming tussen verschillende afdelingen door een team te vormen die bestaat uit de juiste deelnemers:

- Bedrijfsleiders, waaronder CISO's en CIO's. Zij brengen een breder en meer op de lange termijn gericht zakelijk perspectief op de mogelijke gevolgen van databescherming met zich mee.
- Deskundigen op het gebied van compliance en risicobeheersing begrijpen de regelgeving tot in detail en weten hoe databescherming daarbinnen past.
- Mensen met juridische kennis bieden inzicht in potentiële juridische risico's en kunnen helpen bij het correct opstellen van communicatie en overeenkomsten.
- IT-specialisten bieden diepgaande kennis over de huidige bescherming van data binnen het bedrijf, enkele van de meer kritieke problemen met die bescherming en de mogelijke implicaties van verschillende technologische keuzes.

2. BEVORDER EEN CULTUUR VAN VERANTWOORD DATAGEBRUIK

Organisaties passen hun beleid tegenwoordig steeds meer aan thuiswerken aan. Het uitbreiden van die cultuur van databewustzijn buiten de traditionele kantooromgeving wordt essentieel voor het veilig houden van data binnen een verspreid werkend personeelsbestand. Benadrukken hoe werknemers kunnen bijdragen aan een cultuur van beveiliging en waarom dat ze helpt hun werk te doen, is effectiever dan je alleen op beperkingen te richten. Bedrijfsleiders kunnen een voorbeeld vormen voor werknemers op alle niveaus door een mentaliteit voor databescherming aan te nemen en door duidelijk te communiceren dat databeveiliging een strategische prioriteit is.

Deze cultuur van verantwoorde data moet flexibel genoeg zijn om alle werknemers te omvatten, of ze nu thuis of op kantoor werken, en moet ook van toepassing zijn op leveranciers, consultants en andere derde partijen.

3. MAAK JE BELEID SOCIALER EN TRAIN MEDEWERKERS

Als werknemers computerbeveiligings-dreigingen niet kennen of volledig begrijpen, kunnen ze zich niet aan het beleid houden. Bedreigingen van binnenuit, al dan niet opzettelijk, zijn een belangrijke oorzaak van datalekken voor organisaties van elke omvang, en deze inbreuken kunnen kostbaar zijn. Je databeschermingsprogramma kan alleen effectief zijn als beleid dat is ontworpen om dataverlies te voorkomen op alle niveaus duidelijk wordt gecommuniceerd. Als werknemers het programma niet kennen of volledig begrijpen, kunnen ze het ook niet toepassen. Maak het programma makkelijk te vinden en maak het waar mogelijk onderdeel van de dagelijkse productiviteit. Daarnaast moet je zorgen dat databeschermingsbeleid dat in je trainingen wordt behandeld, relevant is voor de werklocaties van je werknemers, of dat nu thuis, op kantoor of allebei is. Effectieve trainingen vereisen duidelijk beschreven beleid voor het voorkomen van dataverlies, ondersteund door regelmatige communicatie en opfrissessies. Trainingen moeten ook voor iedereen toegankelijk zijn, waar ze ook werken, en de trainingen moeten actueel worden gehouden. Ten slotte kun je de effectiviteit van trainingen meten met enquêtes voor en na een training.

4. KIES VOOR PARTNERS MET EEN PROACTIEVE BENADERING VAN COMPLIANCE

Hybride werken leidt vaak tot meer afhankelijkheid van cloudleveranciers voor dataopslag en applicaties.

Voor je databeveiliging is het essentieel dat je communiceert hoe de verantwoordelijkheid voor databescherming tussen jou en je leveranciers is verdeeld. Zorg dat je kiest voor leveranciers die hebben bewezen verder te gaan dan de basisprincipes van databeveiliging. Ze moeten kunnen voldoen aan de behoeften van verschillende afdelingen en bedrijfsonderdelen. Hoe meer compliancefunctionaliteit de leverancier kan verzorgen, hoe meer je je op je bedrijf kunt richten.

5. BEWAAK EN TEST REGELMATIG DE EFFECTIVITEIT VAN JE PROGRAMMA

Beoordeel de effectiviteit van je databeschermingsbeleid en identificeer proactief gebieden met potentiële risico's door voortdurende bewaking en tests. Het is een goed idee om bewaking te beschouwen als een vroegtijdig waarschuwingssysteem dat je waarschuwt voor potentiële data- en beveiligingsproblemen, voordat ze schadelijk worden. In het verleden kostte bewaking veel middelen, maar de vooruitgang in kunstmatige intelligentie en automatisering maken bewaking nu gemakkelijker dan ooit. Door bewakingstaken die anders handmatig zouden worden uitgevoerd te automatiseren, komen er IT-middelen vrij waardoor je teams zich op innovatie kunnen richten. Ze kunnen bedreigingen zo ook sneller en beter herkennen. Met de opkomst van de hybride werkomgeving is het ook essentieel om de bewaking en het testen van externe apparaten en apparaten van werknemers aan te pakken. Door gebruik te maken van technologieën zoals uniforme preventie van gegevensverlies in al je productiviteitsapps en een cloudbeleid voor voorwaardelijke toegang waarmee toegangsrechten tot een minimum worden beperkt, kun je de beveiliging verbeteren zonder de productiviteit te schaden.

6. GEBRUIK GEÏNTEGREERDE TOOLS OM DE EFFICIËNTIE TE MAXIMALISEREN

Het gebruik van verschillende oplossingen voor databescherming voor werken op kantoor of thuis kan de complexiteit vergroten en gaten in je beveiliging creëren. In een recente enquête meldde 59% van de IT-leiders dat er, sinds er op grote schaal thuis wordt gewerkt, meer e-maildata verloren gaan.

Geïntegreerde tools voor datamanagement en –bewaking kunnen je helpen bij het beschermen van data op verschillende apparaten en locaties, waaronder mobiel, cloud, multicloud, multiplatform en lokaal. Met deze tools kun je:

- Datadetectie en -classificatie automatiseren om je te helpen bij de compliance en het risico op lekken te verkleinen.
- Het beheer van netwerkdiensten uitbreiden met zaken als toegang op afstand, apparaatbeheer en back-ups en noodherstel.
- Gevoelige data versleutelen zodat ze onleesbaar zijn voor derden die er toegang toe kunnen krijgen.
- IT-infrastructuur met kwetsbaarheidsscans en patches tegen potentiële kwaadwillenden beschermen.

MEER LEZEN?

Phishing en andere kwaadaardige e-mails

Download

Hiscox: Cyberclaims uit de praktijk

Download

BEDANKT VOOR HET LEZEN VAN DEZE WHITEPAPER. HEEFT U NOG VRAGEN OVER HET ONDERWERP?

Neem dan gerust contact met ons op via info@socured.nl of 020 708 55 65.

Socured
Klokkenbergweg 50A
1101 AP AMSTERDAM-ZO
Tel.: 020 708 55 65
info@socured.nl
www.socured.nl

Onderdeel van Socia

Over Socured

Socured is gevestigd in Amsterdam en is onderdeel van Socia. Socia helpt al meer dan 15 jaar haar klanten op het gebied van IT en heeft inmiddels een mooie voetafdruk achtergelaten bij veel bedrijven in Nederland als het gaat om IT-diensten.