Application de DORA : considérations majeures pour le secteur financier

Tuesday 10 December, 2024

Related Sectors:

Business & Finance :: Computing & Telecoms ::

Scan Me:

Attribué à Sean Tilley, Directeur Commercial EMEA de 11:11 Systems

L'industrie financière est une cible tentante pour les cybercriminels, ce qui a donné lieu à un durcissement de la réglementation pour mieux protéger ces institutions et leurs employés, ainsi que les données des clients.

Les recherches récentes réalisées par Security Scorecard
indiquent qu'en 2023, 78 % des institutions financières européennes ont subi une violation de données impliquant un tiers. D'autre part, 84 % des organisations financières ont été affectées par une violation des données faisant intervenir une quatrième partie. Par conséquent, les régulateurs et les autorités ont à cœur de renforcer les défenses des institutions financières pour contrer les cyberattaques et autres incidents affectant les technologies de l'information et des communications(TCI).

Le futur règlement DORA (Digital Operational Resilience Act), qui devrait prendre effet en janvier 2025, restructure la réglementation de la sécurité des données en obligeant les institutions financières à adopter une approche en amont et multifacettes de la gestion des risques propres aux TIC. Cette réglementation va introduire des règles strictes de protection, de détection, de confinement, de récupération et de réparation en cas de cyber-incidents ou de perturbations technologiques. DORA impose une série de conditions strictes aux entreprises spécialisées dans la finance, telles que la gestion des risques, les rapports d'incidents, la gestion des risques de tiers, les tests de résilience opérationnelle numérique et le partage de renseignements sur les menaces, afin de créer les conditions d'une résilience numérique fiable.

DORA vise à encourager et harmoniser les initiatives d'amélioration de la résilience opérationnelle dans les quelque 22 000 entités financières basées dans l'Union européenne. Cette législation ne se limite pas aux banques, mais touche également les institutions de crédit, les prestataires de paiement, les compagnies d'assurances, les firmes d'investissement, les gestionnaires de fonds, les fonds de pension, les services de crypto-monnaie, les services informatiques de tiers, le crowdfunding et bien plus encore. Ce nouveau règlement permet de jeter les bases de systèmes financiers agiles et prêts à affronter les menaces numériques d'aujourd'hui comme celles de demain.

Risques liés à la non-conformité

L'absence de mise en conformité avec le nouveau règlement expose les institutions financières à des risques graves, notamment sous forme de pénalités sévères, proches de ce qui a été pratiqué pour le RGPD. De plus, ces pénalités peuvent s'accumuler au prorata du nombre de jours de retard, ce qui peut avoir un impact financier majeur et renvoyer une mauvaise image des organisations qui ne prennent pas les mesures demandées.

Par exemple, en cas de cyber-incident, les organisations doivent prévenir les autorités et les parties concernées sous 72 heures. Sinon, les informations relatives à l'incident sont rendues publiques. Quoi qu'il en soit, il est essentiel que les entreprises surveillent constamment leur environnement informatique pour identifier les menaces et les violations, et mettent en place des contre-mesures efficaces. Pour cela, elles doivent implémenter des systèmes de détection avancés, un plan complet de contre-mesures et évaluer de façon très précise les vulnérabilités des systèmes de l'organisation. En l'absence de supervision, les organisations risquent de ne pas voir les signes avant-coureurs d'attaque et de ne pas prévenir les autorités compétentes à temps, ce qui peut encore aggraver la situation.

Choisir des partenaires experts pour mettre en place un cadre de conformité couvrant tous les aspects

En termes de préparation pour ces nouveaux règlements, toutes les organisations doivent procéder à une évaluation précise de la résilience et des lacunes. Cela permet de mesurer le degré de préparation de l'organisation en cas de cyber-incident, ainsi que sa capacité à s'en relever rapidement. Pour cela, il faut procéder à une évaluation poussée des composants clés, ce qui peut inclure l'état actuel de l'infrastructure de sécurité, les capacités de réponse en cas d'incident, ainsi que les efforts quotidiens de surveillance.

Toutefois, y parvenir tout en gérant les activités métier peut être difficile. Par conséquent, il est important de pouvoir compter sur des spécialistes et des prestataires externes capables d'évaluer les capacités de résilience. Ces tiers aident les entreprises à créer une véritable feuille de route de conformité, afin de définir un plan clair permettant non seulement de parvenir à la conformité, mais de la maintenir. Ce plan donne la priorité aux projets qui auront le plus d'impact sur la position de sécurité de l'entreprise et l'atténuation des risques.

Ce processus implique la gestion du temps à consacrer aux différents projets de conformité, ainsi que la mise en évidence des aspects de la cyber-sécurité qui auront l'impact le plus significatif. En s'appuyant sur une feuille de route dressée par des experts, les organisations sont mieux à même de répartir leurs ressources et de traiter en priorité les menaces les plus pressantes.

Stratégies de réponse aux incidents et de responsabilité au niveau de la direction

Le processus de réponse en cas d'incident constitue un composant essentiel de l'évaluation de la résilience. Un plan de crise bien écrit est important, mais la réaction de l'organisation l'est encore plus, ce qui passe par des exercices poussés de gestion des incidents affectant les TCI pour se tenir prêt à toute éventualité. Il est essentiel d'examiner le cadre existant et les procédures de traitement des cyber-incidents, afin de s'assurer qu'ils sont conformes à la réglementation. Cela inclut de déterminer si l'infrastructure interne est en place pour la récupération en cas de cyberattaque et si elle permet de surmonter une attaque majeure.

De plus, il est important de veiller à l'engagement de la direction en cas d'atteinte à la cybersécurité, car cela doit être vu comme une menace existentielle qui demande l'implication de l'équipe de direction et du comité directeur. La sensibilisation de la direction aux risques encourus, et le fait de lui donner un rôle direct de supervision des initiatives de cybersécurité, permet d'instiller une culture de la sécurité à tous les niveaux de l'organisation.

Surveillance continue et gestion du cycle de vie

Le suivi constant des facteurs de risque est essentiel pour maintenir une forte position de sécurité, car ce type de programme peut également être utilisé pour se démarquer de la concurrence.

Aujourd'hui, les cybermenaces évoluent rapidement et pour rester à jour, il est essentiel de gérer le cycle de vie des systèmes informatiques, des protocoles de sécurité et des risques de façon diligente. Les organisations doivent constamment réévaluer leur position en termes de conformité et d'adaptation des processus. Il est important d'adopter une approche de gestion du cycle de vie, à savoir comprendre, planifier, tester et répéter, pour être prêt en cas d'incident de cyber-sécurité, mais surtout, pour surmonter rapidement les situations dangereuses et faire preuve de la résilience que des règlements tels que DORA cherchent à instaurer.

Company Contact:

11:11 Systems

E. 11-11systems@c8consulting.co.uk
W. https://1111systems.com/

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.1111systems.pressat.co.uk