Impact du Brexit sur les identités à forts privilèges

Alors que le Royaume-Uni et le reste de l'Europe se préparent au Brexit (à savoir la sortie du Royaume-Uni de l'Union Européenne), les experts en matière de sécurité des informations se demandent ce qu'il adviendra des procédures de sécurité et de contrôle des risques déjà en place, et comment elles devront s'adapter à la situation émergente. Ce document examine l'impact du Brexit sur la gestion des accès à forts privilèges et les solutions immédiates que les experts en sécurité des informations peuvent envisager pour réduire les risques.

Brexit : que nous réserve l'avenir ?

La remise de la lettre de notification de départ du Royaume-Uni de l'Union européenne (UE) par Theresa May, Première ministre britannique, a marqué le début officiel de la procédure de sortie de l'UE. Cette notification ouvre une période de 24 mois durant laquelle les deux parties devront créer un cadre pour travailler ensemble. Le processus est schématisé dans l'illustration ci-dessous.

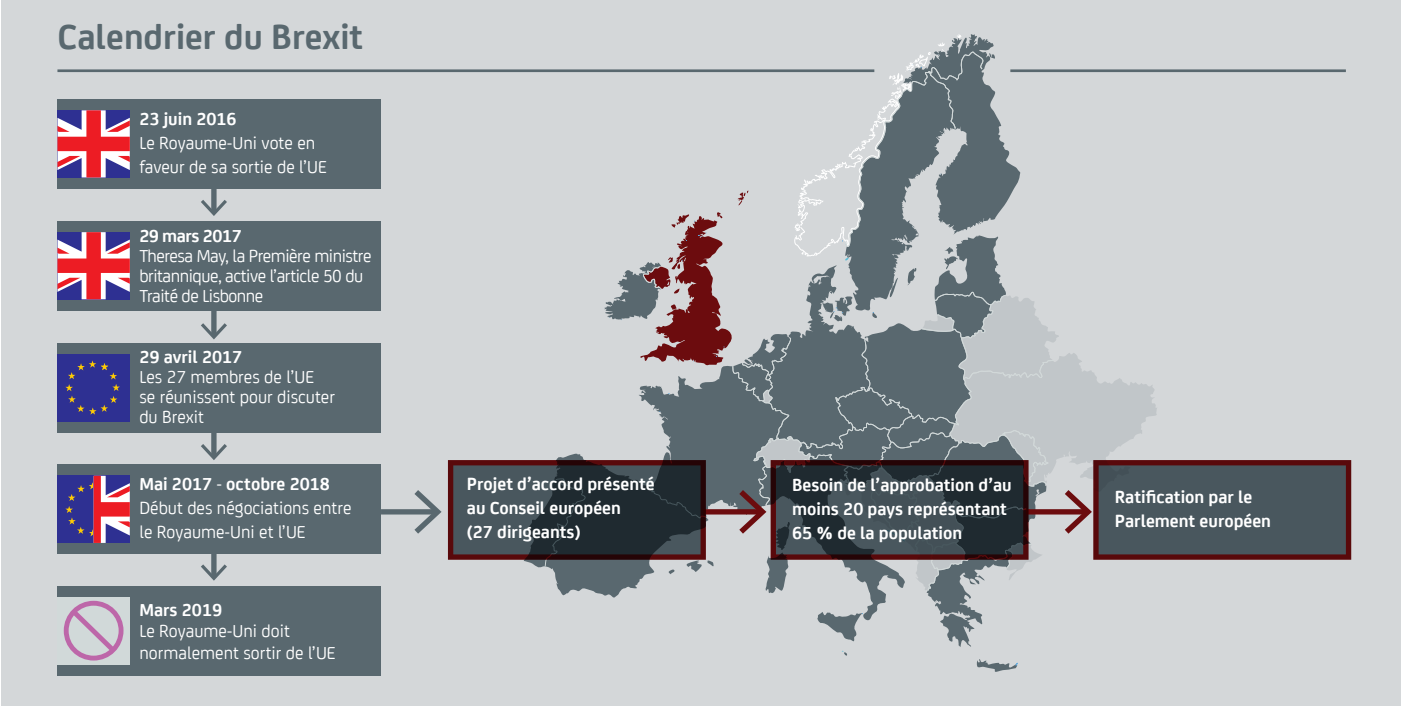

Illustration A. Calendrier du Brexit (avec l'autorisation d'APA et de DW)

Pendant les 24 prochains mois, l'Union européenne et le Royaume-Uni devront se mettre d'accord sur les règles de conduite après la séparation. Pendant ce temps, de nombreuses organisations publiques et privées des deux côtés cherchent de nouvelles façons d'entretenir des relations commerciales fluides. Ce processus est semé d'embûches et de risques. En effet, tous les participants, directs comme indirects, naviguent dans des eaux inconnues. Un programme soigneusement conçu de gestion des risques est donc nécessaire.

Impact économique potentiel

Il existe plusieurs modèles de l'impact macroéconomique du Brexit sur le Royaume-Uni. Plusieurs d'entre eux suggèrent ceci :

- Diminution du PIB sur le long terme
- Baisse de l'investissement direct étranger (FDI)
- Ralentissement de l'immigration

Globalement, cela signifie que de nombreuses organisations devront chercher un moyen de rester compétitives et de continuer à servir leurs marchés respectifs. Pour assurer un minimum de répercussions sur leurs activités, les organisations établissent un cadre pour l'avenir en prenant généralement en compte le scénario le plus défavorable. « À des fins de planification, nous devons nous attendre à un Brexit difficile impliquant que le Royaume-Uni perde son passeport pour l'Union Européenne », écrit James Cowles, PDG de Citigroup Europe, dans une note à son personnel. D'autres institutions financières élaborent des plans similaires, mais elles ne sont pas les seules. Les conséquences pour les deux camps doivent être examinées. À titre d'exemple, Vauxhall envisage d'implanter toute sa chaîne d'approvisionnement pour le Royaume-Uni au sein même du pays, alors que BMW cherche un nouveau site sur le continent pour sa Mini. Cependant, toute décision métier ayant des conséquences sur la main-d'œuvre, tel qu'un déplacement des activités pour améliorer la productivité au sein du Royaume-Uni et ainsi se placer au niveau des autres pays européens ou suite à une modification de la demande mondiale, court le risque d'être étiquetée victime du Brexit.

Conséquence sur les emplois

L'un des sujets de préoccupation est celui de l'impact du Brexit sur les emplois. Plusieurs organisations laissent entendre que des emplois seront délocalisés ; c'est notamment le cas de Nestlé qui a décidé de déplacer la fabrication de son chocolat Blue Riband du Royaume-Uni en Pologne, ce qui correspond à une suppression de 300 emplois pour le Royaume-Uni. Il s'agit peut-être de la conséquence des changements au niveau de l'immigration (renforcement des lois sur les visas ou surveillance renforcée), des droits de douane ou de l'incertitude croissante. Selon l'un des plus grands cabinets de recrutement dans le monde, les embauches dans le secteur privé britannique ont atteint leur niveau le plus bas en trois ans en raison des incertitudes liées au Brexit. Un tel déplacement des emplois a non seulement un impact significatif sur l'économie globale du pays, mais constitue également une menace très importante pour la sécurité des informations.

Exposition aux risques

Comme nous l'avons vu jusqu'à présent, il existe une abondance de preuves démontrant que les organisations doivent gérer d'importants risques dans le cadre du Brexit. Couplée aux changements technologiques profonds que nous rencontrons aujourd'hui, la gestion des risques IT revêt une importance considérable. Une part considérable de ces risques concernent la sécurité informatique. Il a été clairement démontré que les plus grands risques en termes de finances et de marque pour les actifs de sécurité des informations proviennent de l'exploitation des accès utilisateur à forts privilèges. Ce risque s'est amplifié avec l'adoption des environnements Cloud et virtuels par les entreprises pour leur croissance et leur transformation numérique.

Faire face aux risques liés à la gestion des accès à forts privilèges

Alors que les organisations examinent les options qui se présentent à elles pour répondre aux défis que pose le Brexit, en particulier celui du déplacement des employés, elles doivent également s'occuper du risque de menaces internes. Toute incertitude, comme les éventuelles modifications apportées au statut professionnel ou un transfert de responsabilités, peut conduire à des comportements imprévisibles de la part du personnel interne. C'est également une occasion pour une personne malveillante à l'extérieur des entreprises d'exploiter les vulnérabilités potentielles. De plus, un transfert de responsabilités, comme le recours à un fournisseur tiers pour certains processus, peut conduire à une plus grande exposition et nécessitera une supervision et une visibilité appropriées. Ensemble, ces problèmes appellent à la mise en œuvre d'une stratégie efficace orientée sur l'atténuation des risques liés aux accès à forts privilèges. En effet, la protection des données sensibles et de la propriété intellectuelle devient encore plus importante.

Remarques concernant l'atténuation des risques liés aux accès à forts privilèges

Les points suivants doivent être pris en considération pour atténuer le risque lié à la compromission ou l'abus des accès à forts privilèges durant les périodes d'incertitude.

1. **Échelle :** surface d'exposition
    a. Terminaux/périphériques : non limités aux données stockées sur site, mais concernent aussi tous les actifs virtuels ou Cloud
    b. Identités : non limitées aux administrateurs, mais concernent aussi les comptes d'application à application et les scripts

2. **Portée :** future stratégie
    a. Transformation numérique : s'il existe un programme de transformation numérique, intégrez tous les clients, fournisseurs et partenaires participant
    b. Programmes d'Internet des objets (IoT) : pensez à tous les appareils qui pourraient avoir accès à des informations à forts privilèges
3. **Automatisation :** apprentissage machine et enregistrement des sessions
    a. Apprentissage machine : le recours à l'analyse du comportement des utilisateurs (User Behavior Analytics, UBA) permet de détecter les anomalies dans le but de réduire le temps de détection et d'atténuation de l'exposition
    b. Enregistrement des sessions : utile pour la non-répudiation et la mise en conformité
4. **Ressources :** budget et talent
    a. Budget : en raison de l'incertitude géopolitique, il est fort probable que les budgets seront limités pendant la négociation du Brexit
    b. Talent : avec les changements imminents qui concerneront l'immigration et la migration des talents, il sera crucial de s'assurer que le besoin de compétences spécifiques n'entrave pas le déploiement

Conclusion

La gestion des accès à forts privilèges, comme celle proposée par les solutions de CA Technologies, sera un point important pour garantir la protection des actifs critiques durant cette phase de changement géopolitique. Bien qu'il puisse être séduisant de commencer par des fonctionnalités basiques, comme la mise en chambre forte de mots de passe, il est capital d'attaquer le problème de manière globale pour atténuer le risque. Le Brexit suit un calendrier fixe. Le rythme des activités va probablement s'accélérer, laissant ainsi peu de temps aux professionnels de la sécurité des informations pour réagir. Il sera crucial de prendre en compte le coût total de possession (TCO) d'une solution, ainsi que la portée et l'échelle du support fonctionnel avant de s'engager sur ce chemin. Attendez-vous à rencontrer des inconnues comme la séparation des fonctions et des problématiques liées à la souveraineté des données durant le processus. Enfin, réfléchissez à une solution qui vous apportera non seulement l'échelle, la portée et l'automatisation voulues, mais qui agira également comme la fondation d'une gestion sécurisée des accès à forts privilèges, couplée à des analyses pilotées par apprentissage machine. Ce changement géopolitique a non seulement des conséquences sur le Royaume-Uni, mais aussi sur tous les partenaires commerciaux importants du Royaume-Uni et de l'Union Européenne.

CS200-277092_0617