アプリのセキュリティを第一に考える

アプリケーション セキュリティ

GDPRコンプライアンスへの一歩

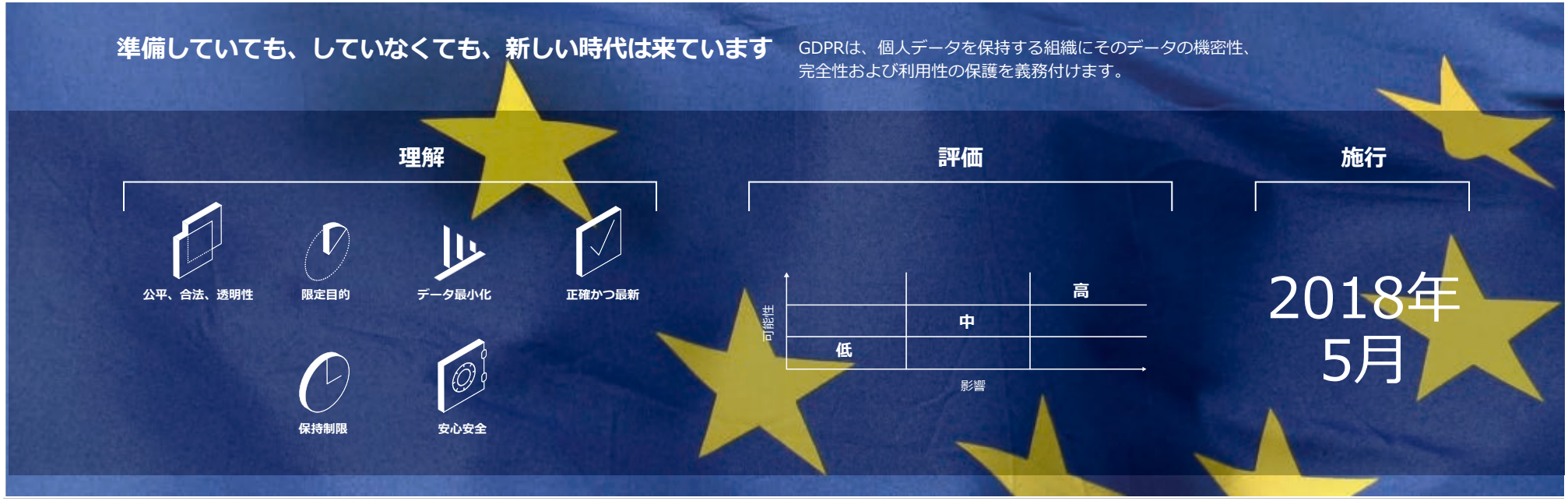
概要

最近まで、複雑なサイバー攻撃のほとんどは、企業の知的財産を盗む、または国防インテリジェンスを高める国家によるものでした。

現在、より巧妙化された情報漏洩問題が報告されていますが、これらは、組織犯罪が関連する金銭目的の攻撃が原因であり、一般的には個人データが被害に巻き込まれています。ますます多くの個人データがアプリケーションで処理および保存され、アプリケーションはサイバー犯罪の第一の標的となっています。組織は、多くのセキュリティ上の理由から、アプリケーションおよびそのユーザーの個人データを保護していますが、間もなくこれに、別のやむにやまれぬ経済的な理由が加わります。それはEU一般データ保護規則（GDPR）です。

2018年5月までに、EUの市民に関するデータを保持または処理するすべての企業は、データ プライバシーに関するGDPRの新しい規則に準拠しなければなりません。GDPRは、個人データを保持または処理する組織にそのデータの機密性、完全性および利用性の保護を義務付けることで、個人のプライバシーを守ることを目的としています。違反に対する罰則は厳しく、いずれかの基本方針（次のページを参照）に違反した場合、罰金として€2,000万、またはすべての年間売上の4%のいずれか高い金額が企業に課せられます。恐らくこれ以上のリスクは、データ保護機関が、組織の個人データ処理に介入および停止でき、これにより日常業務が完全に停止する可能性があるということです。これらの懸念を考慮して、このebookの推奨事項など、企業が新しい法的要件に従うために何をすべきかを弁護士に相談してください。

企業コンプライアンスは必ずしもセキュリティ強化につながるわけではないというのは常套句ですが、GDPR要件を十分に理解した上でアプリケーション保護戦略を設計することは、コンプライアンスへの取り組みだけでなく、セキュリティ プログラム全体にも役立ちます。



概要：
GDPRとは

GDPRは、EUデータ保護条令に置き換わり、EU各国における個人データ保護方法の解釈を統一する新しい法制度です。GDPRは、その基礎原理はEUデータ保護条令と同じですが、その適用範囲が拡張され、具体的には、別の組織の要求に応じてデータを処理する組織、およびそれを管理する組織にも適用されます。新しい規制に従うには、組織は、個人データの処理または管理に関する以下の基本原理に従う必要があります。

公平、合法、透明性

組織は、個人データを収集するための正当な理由が必要になり、透明性のある通信方法に限ってデータを使用する必要があります。個人データ収集は、法的な目的に関連する必要があり、使用事例によっては本人の明示的同意が必要になる場合があります。

限定目的

組織は、データがどのように使用されるかを開示する必要があり、それ以外の目的でデータを使用することはできません。

データ最小化

組織が定める目的に厳密に従わない場合は個人データを収集できません。

正確かつ最新

組織が収集および保存する個人データにはユーザー自身がアクセスできなければならず、その情報の更新を許可する必要があります。

保持制限

データは、組織が定める目的の達成に必要な期間を超えて保存できません。

安心安全

個人情報を収集および保存する組織は、処理システムおよびサービスの機密性、完全性、利用性および耐性を合理的に保護する必要があります。

セキュリティ リスクの評価

従来の組織の境界は分割を続け、ビジネスは、プライベート データ センタまたはパブリック クラウドに置かれるアプリケーションや、SaaSプラットフォームを介して提供されるアプリケーションを利用しています。個人データに関するリスクを評価すると、分析の大部分がこれらのアプリケーションに集中していることがわかります。評価の結果、リスクを軽減するセキュリティ コントロールを開発することになりますが、これらのコントロールの多くには、技術的なソリューションが必要な場合があります。

どこから始めるか

情報セキュリティ リスクは、脆弱性を利用する脅威の可能性および攻撃が成功した場合の影響として適切に算出されます。まず、何を保護すべきかを知る必要があります。組織は個人データをどのように収集、保管および処理しているか。どのようなビジネス プロセスがそれを支えているか。どのようなシステムが個人データを扱うか。サード パーティが個人データを処理することがあるか。そして、最も重要なことで、このデータを公開することにより個人の自由にどのような影響があるか。

影響の評価 アセット（データ、システム、プロセスなど）を確認したら、影響を評価できます。評価するには、仮想の障害または情報漏洩と機密性、完全性および利用性の概念を結び付けます。たとえば、WebサーバがDoS攻撃を受け、顧客が個人データにアクセスできなくなる障害が発生する可能性があります。機密性、完全性、利用性への影響は、潜在的な有害事象に従い、それぞれ「低」、「中」、「高」と評価できます。これにより、個人データ、または個人データを保存するシステムへの攻撃が成功した場合の影響を簡単かつ効果的に考えることができます。

脅威モデリング 次のステップは、脅威モデリングです。これは、自然の脅威および敵対的な脅威がアセットに影響する可能性を測定するプロセスです。Verizon Data Breach Investigations Report[1]やF5 Labs[2]などの情報機関が提供する脅威インテリジェンスを常に意識することで、攻撃の傾向を把握できます。また、攻撃者の動機を考えることで、効果的な脅威のリストを作成しやすくなります。また、使用されるエクスプロイトの種類に応じて脅威を分類するSTRIDEなどの分類手法も役に立ちます。[3]STRIDEは、Spoofing identity（なりすまし）、Tampering with data（データ改竄）、Repudiation（否認）、Information disclosure（情報漏洩）、Denial of service（サービス拒否）、Elevation of privilege（特権の昇格）の頭文字をとった頭字語です。このような取り組みにより、アプリケーション クラウドが失敗する、または情報漏洩の被害に遭う可能性のある、考えられるあらゆる方法をリストできます。

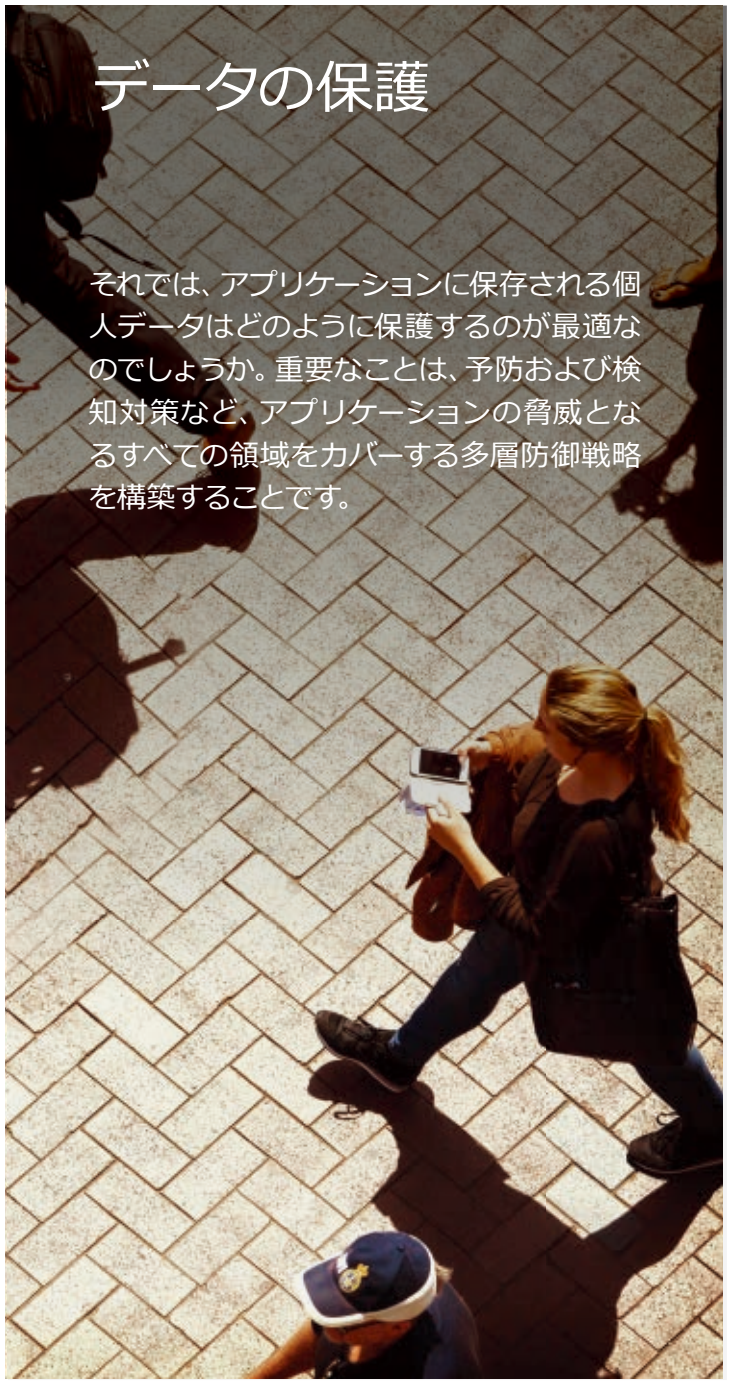
脆弱性スキャン 次のステップは、アプリケーションのどの部分が脅威アクターによる攻撃に脆弱であるかを評価する、脆弱性スキャンです。潜在的な攻撃ベクトルを見つけることは困難です。そのため、自動化されたスキャン、静的コード分析、手動による侵入検査など、できるだけ多くの方法を利用して、脆弱性をテストすることをお勧めします。

リスク モデリング 最後のステップは、リスク モデルを作成して、リスクにスコアを付けることです。これにより、実施する対策への取り組みのためのリソースに優先順位を付けることができます。量的および質的のリスク評価には多くの方法がありますが、最も時間をかけずに、最も大きな効果を生み出す最適な方法は、攻撃の可能性と攻撃が成功した場合の影響に関する客観的な意見に基づいて脅威を評価することです。

[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[2] https://f5.com/labs
[3] https://www.owasp.org/index.php/Threat_Risk_Modeling#STRIDE

STRIDE

SPOOFING IDENTITY（なりすまし）、TAMPERING WITH DATA（データ改竄）、REPUDIATION（否認）、INFORMATION DISCLOSURE（情報漏洩）、DENIAL OF SERVICE（サービス拒否）、ELEVATION OF PRIVILEGE（特権の昇格）



情報漏洩の可視化

課題

GDPRが規定する情報漏洩時の72時間以内の通知規則により、ネットワーク トラフィック内の脅威を見抜くことが重要になります。攻撃者は、SSL/TLSを使用して転送時の攻撃ペイロードを暗号化することで、暗号化されたトラフィックに気付かない侵入防止システム（IPS）およびデータ損失防止（DLP）ソリューションなどの検査デバイスを回避できます。これらのデバイスのほとんどは、トラフィックを復号化できないか、復号化できてもデバイス自体が事実上利用できなくなるほどのパフォーマンス ヒットが生じます。

暗号化の暗号がますます高度になるにつれ、この問題は拡大しています。完全前方秘匿性を提供する暗号は、最も強力なセキュリティを提供しますが、各デバイスのCPUリソースに大きな負担となります。

GDPRが規定する情報漏洩時の72時間以内の通知規則により、ネットワーク トラフィック内の脅威を見抜くことが重要になります。

解決策

復号化されたトラフィックのストリームを一度に1つではなく、並行して各検査デバイスに送信できる「サービス チェイニング」を実現するソリューションを実装することで、トラフィックのフローを余計に遅延させることなく、迫り来る脅威を可視化できます。また、トラフィックの種類に基づいて、通過する検査デバイスをインテリジェントに選択することで、各デバイスのCPUサイクルをより効率的に使用できるソリューションもお勧めします。より多くのCPUサイクルを利用できることで、通過時間が改善されます。

このアーキテクチャには、復号化および再暗号化を一元管理できるという、もう1つのメリットがあります。インターネットの50%が暗号化されている現在[4]、暗号化されたトラフィックを可視化できることは、ほとんどの組織にとって不可欠になっています。

[4] https://f5.com/labs/articles/threat-intelligence/ssl-tls/the-2016-tls-telemetry-report-24674

アクセス制御

課題

インターネットと接するアプリケーションは、悪意のあるアクセス試行などの脅威と直面しますが、認証および認可は、すべての状況に対して許可するかしないかを決定するだけの単純なことではありません。アクセス決定は、ユーザー ロール、データの重要性、エンドポイントの状況など、多くのリスク要因に基づいて行う必要があります。

また、平均的なユーザーにより使用される膨大な数のアプリケーションは、ユーザーのパスワード管理業務に大きな影響を与えているため、ログイン認証情報は再利用されるか、その安全が損なわれています。特権ユーザーが企業システムおよび個人データにどのようにアクセスするかを考慮し、簡単なパスワードでも必要なセキュリティ レベルを満たせるかどうかを判断してください。

解決策

アクセス ゲートウェイを一元化することは、安全な認証を管理する優れた方法です。強力なネイティブ認証のないアプリケーションでも、ゲートウェイにより追加できるSAMLまたはOAuthなど、安全な認証フレームワークを利用できます。これにより、すべてのアプリケーションにシングル ポータル（およびシングル パスワード）で安全にアクセスできるので、ユーザー エクスペリエンスが向上します。

また、現在の脅威環境では必須となっている、多要素認証も簡単に導入できます。限られたセキュリティ リソースを単一のアクセス決定および施行ポイントに集中させることで、アプリケーションにより収集される個人データの機密性および完全性を保護できます。

アプリケーション保護

課題

最近の最大の情報漏洩のいくつかはアプリケーションの脆弱性が原因であることから、間違いなく、アプリケーションは、価値ある個人データを盗むことを目的としたサイバー犯罪の標的にされています。Webアプリケーション攻撃の93%は組織犯罪に起因し、そのうち77%にボットネットが関与していて[5]、サイバー犯罪は今後も拡大するビジネスです。アプリケーションおよびそこに保存されるデータを保護することは、あらゆるセキュリティ戦略に不可欠なことですが、2018年に施行されるGDPRを考慮すると、これはさらに重要になります。冗長性および効果的なフェイルオーバー戦略は、可用性を維持する上で重要なことです。

しかし、DDoSの「booter」および「stresser」は、ボタンを押すだけで多くの組織のWebプロパティおよびサービスをダウンさせ、データを利用不能にする安価なツールとして商品化されています。DDoS攻撃は初心者でも実行できるほど簡単なので、GDPRに違反するリスクは重大です。

解決策

最新のWebアプリケーション ファイアウォール（WAF）は、アプリケーションを保護するだけでなく、OWASP Top 10[6]の脆弱性や、感染したクライアント接続からのクレデンシャル スタッフィングまたはインジェクション試行に対する防御にも役に立ちます。WAFは、行動分析を実行して、正当なユーザーからの接続を許可し、ヘッドレス ブラウザまたはマルウェアによる自動化された接続またはインジェクション試行を拒否できます。

また、効果的なWAFは、一般的になりつつあるアプリケーション レベルのDDoS攻撃を検知および停止できます。包括的なDDoS保護として、マルチベクトル攻撃を検知および阻止できるオンプレミス ソリューションに加え、アップストリーム プロバイダにより攻撃トラフィックをネットワーク到達前にスクラブすることで、大規模な大量攻撃を回避できるハイブリッド ソリューションについて検討してください。

[5] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[6] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

GDPRコンプライアンス
セキュリティのために

準備していても、していなくても、新しい時代は来ています。組織は、新しいGDPRフレームワークに準拠できるようにそのセキュリティ プログラムを評価する必要があります。組織が取り組むべき問題は山積みなので、リスクが最も高い分野に焦点を置く必要があります。関連性があり、実用的な脅威インテリジェンスの利用を含め、優れたリスク管理プロセスにより、発生する可能性が最も高い脅威から個人データを保護することにさらに集中して効率的に取り組むことができます。組織が新しいEU規制に準拠するように備えることで、セキュリティ戦略全体を改善しながら、ユーザーの個人データの機密性、完全性および利用性を保証できます。

脅威インテリジェンスの利用を含め、優れたリスク管理プロセスにより、個人データを保護することにさらに集中して効率的に取り組むことができます。

アプリのセキュリティを第一に考える

常時稼働、常時接続のアプリは、ビジネスを強化および変革する一方、ファイアウォールに保護されないデータへのゲートウェイにもなり得ます。ほとんどの攻撃はアプリ レベルで発生しているため、ビジネスを推進する機能を保護することは、攻撃を受けるアプリを保護することにつながります。

F5ネットワークスジャパン合同会社

東京本社
〒107-0052 東京都港区赤坂4-15-1 赤坂ガーデンシティ19階
TEL 03-5114-3210 FAX 03-5114-3201

西日本支社
〒530-0012 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階
TEL 06-7222-3731 FAX 06-7222-3838

お問合わせ先： https://f5.com/jp/fc/

EBOOK-SEC-169957258 | 10.17