セキュリティ、リスクおよびガバナンス

デジタルトランスフォーメーションの基盤

An IDC InfoBrief, *Sponsored by Micro Focus* | **April 2020**

By Chris Kissel, Research Director, Global Cybersecurity Products, IDC

IDC | ANALYZE THE FUTURE

US46217520TM

企業にとって、デジタルトランスフォーメーションは必須である

IDCでは、デジタルトランスフォーメーション（DX）は、次の3段階のフェーズから成り立つと考えている。

新しいテクノロジーとデリバリーモデル

プラットフォームとコミュニティ

自律型システム

新しいデジタルエコノミーは、4つの本質的要素からなる。

1. **自動運転における搭乗者に関する課題（安全性など）**
2. **マイクログリッド**
3. **ラストマイル**
4. **オープンバンキング**

DXは、新しいテクノロジーと既存プラットフォーム改善の統合的アプローチを含む。IDCでは、世界的な進展から見て、現在は第2フェーズへの移行期であるとも考えている。

以下は、IDC Global DX Leaders Study (2019年6月) の調査結果である。

63% DXに出遅れ「統一された戦略と取り組みが見られない」組織（Digitally Distraught）の割合

22% 現在のDXの取り組みは短期的な解決策として設計されていると回答した組織の割合

12% 多くの取り組みは「場当たり的」で組織全体の方針として位置づけられていないと回答した組織の割合

DXは、セキュリティやコンプライアンスの観点では、「プッシュ・プル」型の活動と言える

- ニュートンの第3法則は、「物体に力（作用）を加えると、真逆の方向に同等の力（反作用）を受ける」としている。DXにおいて俊敏性を目指す企業は、概して同様の状況に直面する。
- モバイルやソーシャルメディアは、顧客エクスペリエンス（CX）を向上させる。だが、これらのテクノロジーに対して従来のセキュリティ統制を適用することは難しい。IoT（Internet of Things）も問題になる。
- コンプライアンスは難題である。EU一般データ保護規則（GDPR）は、重大な違反に対し、企業の全世界売上高の最大4%の制裁金を科すことができる。
- 違反が発生する可能性のある領域は、アイデンティティの取り扱い、「忘れられる権利」、データ主権、伝送中や保存中のデータの暗号化、サイバーセキュリティ体制である。

モダンな企業のための適切かつ包括的なセキュリティ体制の実現

- **異種混合ネットワークは、セキュリティの状況を変化させている**
- **権利やアイデンティティは劇的な変化を遂げ、ITチームやセキュリティチームは、後れを取らずにデータの安全性を維持するために苦労している**
- **顧客や契約者は、ネットワーク相互性の拡大によって、俊敏性を手にできたが、アイデンティティやアプリケーションの関連では新たな脆弱性が生じている**

許容可能なサイバーセキュリティ体制を実現しようとすると、さまざまな問題に直面する。

- 顧客とやり取りする場合、顧客は依然として、個人を特定できる情報（PII）に対する権利を有している。
- セキュリティチームは、構造化データや非構造化データの所在場所を突き止める必要がある。そして、データの安全性を維持し、その利用についてはアクセス権の保有者のみに制限しなければならない。
- コンテナについては、バグへの対処として、繰り返し利用されるコンテナイメージへのスキャンが必要である。
- 現在のネットワークでは、デバイスの多様化と同時にネットワーク自体の相互接続によって複雑性は際限なく増大する。そうした状況の中で、すべてのアイデンティティの管理と、そのアイデンティティごとのデータへのアクセス権が、厳格かつ高い利便性を持って維持されなければならない。
- ネットワーク上に新たにデバイスが追加されると、その複雑性は幾何級数的に拡大する。スマートアナリティクスのアプローチを採用することで、データの一貫性が維持されるため、不整合が原因で発生するアラートを抑制できる。

データセキュリティの検討事項

- **検出：** データは、オンプレミス、オフプレミス、サーバーアレイのいたるところに保存可能である。したがってそれらを検出できる能力の存在は不可欠である。
- **分類：** 構造化データと非構造化データは分けて取り扱う必要がある。データの分類は、適切なコンプライアンス管理のために重要である。
- **暗号化：** データは、保存中も伝送中も暗号化しなければならない。
- **難読化：** データの難読化が適切であれば、匿名化や照合によってインサイト（知見）を得ることが可能となる。悪意を持つ者がアクセスしたとしても、難読化された記録しか得られない。
- **データアクセス管理：** データアクセス制限は、データ自体の保護と同様に重要である。
- **データライフサイクル管理：** 真のライフサイクル管理は、アナリティクスのためにどのデータをセグメント化するか、データ保存先をどこに割り当てるか、いつ、いかに適切にデータを破棄するかを含む。
- **コンプライアンス：** データの作成から破棄に至るまで、コンプライアンスの実証とデータのガバナンス確保は不可欠である。
- **ファイル分析：** ファイル分析ソフトウェアは重要である。ファイルの完全性はエンティティ間の法的拘束力を持つ。もしファイルが改竄された場合、アプリケーションで排除可能である。ファイル改変や人為的改変は、セキュリティ侵害インジケーター（IOC：Indicator of Compromise）となる。

なぜアプリケーションセキュリティは重要なのか

- アプリケーションはDXを加速させる。IDCでは、2024年までに、マイクロサービスの数が5億件になると推定している。
- 組織は完全なリリースオーケストレーション手順を定める必要がある。それによって、署名と認証によって、アプリケーションが実際の本番環境にデプロイされるようになる。
- アプリケーションやマイクロサービスを構築するためには、企業は、カーネルレベルの静的アプリケーションセキュリティテスト (SAST) と動的アプリケーションセキュリティテスト (DAST) の両方の厳格なテスト実施が必要になる。
- 実稼働後にアプリケーションの問題に対処しようとすると、実稼働前の修正に比べ、コストは10倍以上高くなる。

エンドポイント保護はそれ自体ダイナミックである

- セキュリティは、あらゆる種類のエンドポイントとプラットフォームに渡って、接続の最初の段階で最適化され、自動的に適用されなければならない。
- エンドポイントセキュリティにとって、サイバーセキュリティとプライバシーは一体である。
- エンドポイントの可視性は、サイバーセキュリティの根本的懸念材料である。メモリーやレジストリーに変更が加えられた時はIOC発生の可能性があり、ゼロデイ攻撃の兆候とみるべきであろう。

次世代セキュリティオペレーションセンター(SOC)内での多様性の強化

サイロ化したエンドポイント保護は、セキュリティの空白を増大させる。攻撃対象領域の最小化、適応型脅威対策、ガイド付きのインシデント対応、脅威ハンティングなどは、オーケストレート化されたソリューションの要素として組み込まれるべきである。そして、脅威やビジネス課題に対してカスタマイズされ、かつ、リアルタイムに状況を把握して防御すべきである。

セキュリティインフラストラクチャは大きな課題である。テクノロジー、チーム、脅威インテリジェンスが適切に統合されていない場合、組織は以下の能力を失う。

- 脅威の監視と誤検出の減少
- 攻撃への防御
- 脅威の増大と多様化に向け、俊敏にスケールすることで脅威に対抗
- 修復とコストの問題に対応した後の、ネットワーク安全性の確保

SIEMは、オーケストレーション、自動化、ITチケット発行、ケース管理の中心となるべきである。

マイクロフォーカスについての検討

侵害に対する防御をサポートし、DevOpsとSDLCプロセスを保護し、そして個人とそのデータのプライバシーを保護し、さらにエンタープライズレベルで世界的なコンプライアンスの動きに対応できるベンダーはほとんどない。マイクロフォーカスは、セキュリティ、リスクおよびガバナンスに幅広く対応した統合的ソリューションを擁し、この分野における深い知見とアナリティクスと組み合わせることで、将来に向けてデータ、アイデンティティ、アプリケーションを保護する包括的アプローチを採用し進化する組織を支援できる。

- アプリケーションの場合、Fortify STATは、実稼働前にコードが書かれた時点で、コードを監視できる。Fortify on Demand（DAST）は、スキャン実行によって、実稼働後にコードのバグを発見できる。
- アプリケーションの機能テストも、実稼働前に実施できる。

エンドポイントとSOCにおけるセキュリティの促進

- サイバーセキュリティには、適切なジョブに対応する適切なツールが必要になる。
- SOCアナリティクスを通じて、マイクロフォーカスは、最適なセキュリティ体制は人間と機械（マシン）の強力な連携から生まれると確信している。
- ArcSightは、SIEMのバックボーンとなり得る。そして、Intersetのアナリティクスは、信頼性のあるインシデントアラートや有意義なインサイトの提供、ルールベースの検出やロールベースの検出を超えた異常検出を支援できる。Intersetは、教師なしの機械学習（ML）の使用によって、アイデンティティ全体で正常状態の追跡や誤検出の除去を実施し、SOCアナリストが本物の脅威に注力できるよう支援する。ArcSightとIntersetを併用すると、SOCアナリストや脅威ハンターにとって、調査対象候補の特定やアラートの改良に役立つ。
- エンドポイント保護で、以下をすぐにも実現可能である。
  - エンドポイントコントロールの適用（ゲストネットワークへの配置、サンドボックスでの切り離し、またはオフライン化や再イメージ化）
  - アクセス特権の無効化
  - ユーザーに対する再認証依頼
- NetIQは、疑わしいセッションをシャットダウンできる。
- エンドポイントセキュリティとして、マイクロフォーカスにはZENworks Endpoint Security Managementがある。

課題

- マイクロフォーカスの製品は、エンタープライズDevOps、ハイブリッドIT管理、セキュリティ、リスクおよびガバナンス、予測的アナリティクスに対応している。
- セキュリティでは、マイクロフォーカスのツールは他のプラットフォームと独自のプラットフォームを統合した場合と同等の有効性を発揮するのか、つまり、他のツールと共に利用しても問題ないことを確認すべきである。現在、製品間統合が多数利用可能であり、ロードマップではさらに計画されている。
- 同社のツールは、エンタープライズレベルのアプローチのために設計されているが、中小規模のセキュリティオペレーション向けには設計されていないかもしれない。
- マイクロフォーカスは、CI/CDパイプラインでコード保護を開始し、SIEMやデータ保護を通じてプロセスを追跡している。考慮すべき点は、このプラットフォームが、IoTや5Gブロードバンドといった新規の手段に適合できるかどうかである。

データ保護やデータ難読化は、セキュリティ上必須である。しかし、データの匿名化とアナリティクスの適用は、予測的アナリティクスに役立つ。マイクロフォーカスは、データ保護とデータ活用の紙一重の所を進まなければならない。

真のエンドツーエンドエンタープライズ保護は考え方の問題である

- 新たなネットワークの境界は、アイデンティティ、アプリケーション、データである。
- 企業は、各コンポーネントを保護するツールを用意しつつ、以下の多面的な戦略を実現しなければならない。
  - DevOps環境での保護を開始
  - データ検出とデータ保護を重視
  - アプリケーションを監視
  - エンドポイントを保護
  - MLや自動化を活用して、SOCの調査プロセスを最適化
- アイデンティティは、人間、デバイス、サービス、IoT、Webサイトを含むが、これらはごく一部の例にすぎない。権利の概念は、非常に早く変化するため、ITやセキュリティチームにとって、データの安全を維持しながら最前線に立ち続けることは極めて難度が高い。
- 企業は、コンプライアンス、データ、エンドポイント、アイデンティティ、アプリケーションについて、これらは組み合わされた、かつ継続的なものと捉えるべきである。

スポンサーからのメッセージ

マイクロフォーカスによって、以下のことが可能になります。

- インシデントの特定、保護、検出、対応、復旧によって、全体的なリスクプロファイルを軽減でき、また安全かつ最新のITエコシステムを構築できます。
- データプライバシーの維持やデータ侵害、そしてアプリケーション侵害の影響緩和と、脅威の監視によるコンプライアンス監査の可視性確保を実現できます。
- 有効なリスク管理手法をあらゆるレベルで適用できるため、責務と説明責任に関する可視性の強化で経営層や意思決定者を支援し、コントロールを自動化できます。
- データやアイデンティティのガバナンスポリシーの適用、データ侵害の検出と対応、バックアップと復旧の最適化が可能となり、最終的には、使用中、伝送中、保存中のデータを保護できます。
- わずか1日で、アプリケーションセキュリティへの取り組みを開始でき、必要に応じて規模を拡大できます。

マイクロフォーカスは、機微なデータの検出と保護、高度な脅威の検出、および顧客の将来へのセキュリティ体制の適応と進化を支援することに精通しています。

詳細に関しては、https://www.microfocus.com/ja-jp/trend/security-risk-governance をご覧ください。

MICRO FOCUS