ホワイトペーパー

セキュアバイデザイン (セキュリティを基盤とした設計):サイバーセキュリティを基盤に組み込む

この考え方が重要な理由と、製品内部からアタックサーフェスを縮小する仕組み

SOPHOS

エグゼクティブサマリー

セキュアバイデザインは、セキュリティを後付けではなく、基本的な要件として捉えるソフトウェア開発の理念です。

セキュアバイデザインでは、製品を作り上げた後にセキュリティ対策を付け足すのではなく、アーキテクチャや設計からコーディング、テスト、デプロイ、保守に至るまで、開発ライフサイクルのあらゆる段階にセキュリティの考慮事項を組み込むことが求められます。

基本的な考え方はシンプルです。最初から安全に開発すれば、ユーザーは適切な設定方法を理解している場合や、後からセキュリティの欠陥が修正された場合だけでなく、デフォルトで保護されるようになります。

実践的には、ユーザーやプロセスに必要最小限のアクセス権だけを付与する最小権限、製品を最初から最も安全な設定で提供する安全なデフォルト設定、１つの失敗が致命的にならないよう複数のセキュリティ対策を重ねる多層防御、そして安全な言語・フレームワーク・設計パターンを用いて脆弱性全体を排除するといった原則を採用することを意味します。

基本的な考え方はシンプルです。

最初から安全に開発すれば、ユーザーは適切な設定方法を理解している場合や、後からセキュリティの欠陥が修正された場合だけでなく、デフォルトで保護されるようになります。

セキュアバイデザインのアプローチが導入された理由

何十年もの間、テクノロジー業界の多くの企業は「まず製品を出荷し、問題は後で修正する」というモデルで動いてきました。その結果として、サイバーセキュリティは単なるコストセンター、つまりリリースを遅らせ、開発者のフラストレーションを高める存在として見られることが多くありました。その影響は今まさに現実のものとなっており、絶え間ない脆弱性の公開、緊急のパッチ適用、そして何億ものユーザーの個人情報をさらし、組織から数十億ドルを奪う侵害が続いています。

Ivanti Connect Secure の脆弱性、広く使われているオープンソースライブラリにおける Log4Shell の悪用、そして MOVEit Transfer の脆弱性は、いずれも「後付けのセキュリティでは、明確な意図を持つ攻撃者には到底追いつけない」ことを示しました。

この不均衡を認識し、米国のサイバーセキュリティインフラセキュリティ庁 (CISA) は国際的なパートナーとともに、2023 年に「セキュアバイデザイン」に関する正式なガイダンスを発表し、テクノロジー製造企業に対して、顧客のセキュリティ成果に責任を持つよう強く促しました。

セキュアバイデザインの原則では、セキュリティの負担は製品を作るベンダー側が負うべきであり、それを利用するエンドユーザーに押しつけるべきではないとされています。これにより、ベンダーによるテクノロジー製品のセキュリティに対する姿勢が変化し、議論の焦点は「ユーザーが迅速にパッチを適用すべきだ」という利用者個人の責任から、「ベンダーは初めから安全な製品を提供すべきだ」という製造者側の責任へと移りました。

セキュアバイデザインがサイバーセキュリティソリューションにとって最も重要な理由

セキュリティツールでさえ時に攻撃の入口になっています。 しかし、このような事態は驚くほど頻繁に起こります。

これは、多くの組織にとって重大な弱点です。境界型のデバイスが一度攻撃にさらされると、攻撃者は完全に保護されるまで繰り返し狙ってきます。ファイアウォールやその他の境界システムは、修正が提供された後であっても脆弱なままであることがあります。ソフォスが対応した最近のインシデントを分析したところ、確認された脆弱性のすべてで、ベンダーがアドバイザリやパッチを公開してから攻撃者がその脆弱性を悪用するまでの中央値は 322 日でした。つまり、攻撃者にとってほぼ 1 年にわたる攻撃の機会があったことになります。サイバーセキュリティベンダーは、ユーザーが迅速にパッチを適用することを想定していません。

特権的立場の問題

サイバーセキュリティツールは、組織のインフラの中で最も重要かつ機密性の高い領域を担っています。エンドポイントの脅威検知エージェントはカーネルレベルの権限で動作します。SIEM プラットフォームは、すべてのシステムからログを取り込みます。アイデンティティプロバイダーは、すべてのアカウントの鍵を管理しています。ファイアウォールは、信頼されるネットワークと信頼されないネットワークの境界に配置されています。

セキュリティ製品が組織の防御の中心で利用されている場合、それらの製品はセキュアバイデザインの原則を遵守するという、より高い責任を負うことになります。セキュリティ業界のベンダーは、顧客を保護する上で重要な役割を担っており、顧客の信頼は、製品が慎重かつ安全に設計・開発されていることへの期待とセットになっています。

この特権的な立場にあるため、セキュリティ製品に脆弱性がある場合、製品だけでなく、その製品が保護することを意図していたあらゆる対象を危険にさらすことになります。例えば、EDR (Endpoint Detection and Response) エージェントが攻撃者に侵害されると、単に 1 つのツールが掌握されるだけでなく、最も高い権限を持つエンドポイントが乗っ取られることになります。VPN アプライアンスの脆弱性は、単にリモートアクセスが保護されなくなるだけでなく、攻撃者にあらゆる境界型防御を迂回する直接的なトンネルを与えてしまいます。

セキュアバイデザインが無視されるときに起こること

セキュアバイデザインの原則を無視した場合の影響は詳細に文書化されており、適切に従わなければ、企業やユーザー、さらにはインターネット全体の安全性が低下します。

- **セキュリティ侵害のコストが増大します。**製品リリース後に脆弱性が発見された場合、開発時に脆弱性を解決するよりも膨大なコストがかかります。

- **信頼の崩壊。**顧客、規制当局、パートナーは、セキュリティインシデントを繰り返す組織を信頼しなくなります。評判の損失は、技術的な修復よりも何年も長く尾を引くことがあります。

- **規制上および法的なリスク。**世界中の政府がサイバーセキュリティへの規制を強化しています。例えば、欧州連合のサイバーレジリエンス法では、欧州で販売されるデジタルテクノロジーを利用する製品に必須のセキュリティ要件を課しています。セキュアバイデザインの原則を無視する組織は、コンプライアンス違反、罰金、市場からの排除などのリスクを負うことになります。

- **国家安全保障上のリスク。**電力網や浄水場、医療システムなどの重要インフラは、インターネットに接続されたデバイスやシステムにますます依存するようになっています。これらの環境でデフォルトで安全性が確保されていない製品は、国家が支援する攻撃者やランサムウェアオペレーターから攻撃を受ける隙を与え、日常生活にまで深刻な影響を及ぼす恐れがあります。

- **永遠に終わらないパッチ対応への疲れ。**安全な基盤がなければ、組織は受け身的なループに陥ります。脆弱性のスキャン、パッチの優先順位付け、アップデートのテスト、修正の展開を繰り返す必要があります。詳細なサイバーセキュリティ調査に充てることができるリソースが消耗します。

セキュアバイデザイン ファイアウォールの選び方

次回購入するファイアウォールを評価する際には、本当にセキュアバイデザインに基づいて設計されているかを確認することが最優先事項となるべきです。しかし、ベンダーのマーケティング情報に踊らされず、実際の機能を正しく理解するのは簡単ではありません。以下の基準は、本当にセキュアバイデザインの原則に基づいて設計されたファイアウォールを選定する際に、注目すべき主要な特性を見極める手助けとなります。

1. 堅牢化されたアーキテクチャ

ここまで説明してきたように、ファイアウォールのアーキテクチャは、コードレベルから中心機能まで、セキュアバイデザインに基づいていることが極めて重要です。しかし当然ながら、特定のファイアウォールベンダーが自社製品をどの程度強化しているのかを知るのは非常に困難です。多くのベンダーは自社製品の安全性を強調しますが、最終的にその真価を示すのは、直近の実績にほかなりません。

必ず確認すべき項目は以下のとおりです。

- ファイアウォールのすべての領域 (管理、VPN、ポータル) で多要素認証 (MFA) をサポートしていること。
- ZTNA (ゼロトラストネットワークアクセス) の統合をサポートしており、リモートアクセス VPN を排除できること。
- SSH やインターネットからのデバイスへのリモートログインを必要としない安全なリモート管理が実装されていること。
- インターネットに接続されている場合、堅牢化およびコンテナ化されたユーザーポータルを利用できること。
- リリースノートの最近の更新には、セキュアバイデザインの原則に取り組んでいることを示す説明があること。

2. ダウンタイムなしでの脆弱性への自動パッチ適用

ネットワークインフラに対する最大の攻撃方法の 1 つは、パッチが適用されていない脆弱性です。脆弱性が発見されてから実際にパッチが適用されるまで数週間かかる場合があります。多くのユーザーは、次々と登場するパッチを適用し続けなければならず、そのたびに発生するダウンタイムを受け入れることを強いられるため、いわゆる「パッチ疲れ」に陥っています。

ダウンタイムを必要としない自動的な OTA アップデートを提供するベンダーの製品であれば、業務を効率化し、システムに迅速にパッチを適用できます。「自動更新」を謳った広告に惑わされることなく、その「自動」が何を意味するのかを確認してください。アップデート後も再起動が必要であり、ダウンタイムが発生する場合は、「自動」ではありません。

3. 設定リスクの自動監査

セキュリティインシデントのもう 1 つの一般的な要因は、ファイアウォールの設定ミスです。残念ながら、多くのファイアウォールは誤った設定になっていることを知らせてくれず、その結果、悪用されるギャップを生み出しています。次に導入するファイアウォールには、重要な設定を自動かつ継続的に監査され、リスクの高い設定を明確に示し、簡単に対処できるようにする機能を求めるべきです。

4. ベンダーによるプロアクティブな監視

ほとんどのファイアウォールは攻撃を受けても、手遅れになるまで気づけないのが現実です。 幸い、すべてのファイアウォールがそうというわけではありません。攻撃の初期段階で侵害の兆候を検知できるよう、自社製品をリモートで監視し、テレメトリを収集するベンダーを選ぶ必要があります。ベンダーは、異常な活動が検知された際に、迅速に製品を利用している組織やサイバーセキュリティパートナーへ連絡し、攻撃の特定と対処を支援できるだけの意欲と能力を備えているべきです。

5. セキュアバイデザインに取り組むベンダー

言うまでもありませんが、ここまで読んでいる読者の方は、セキュアバイデザインの原則に真剣に取り組んでいるベンダーをすでに思い浮かべているかもしれません。しかし、彼らの言葉をそのまま鵜呑みにしないでください。最近の実績、取り組みの報告、リリースノートを詳細に確認し、どれほど本気でセキュリティに向き合っているのかを見極めてください。

セキュアバイデザインに対するソフォスの取り組み

2024 年 5 月 8 日、ソフォスは米国サイバーセキュリティインフラセキュリティ庁 (CISA) のセキュアバイデザインの取り組みにコミットした最初の組織の一つとなりました。この取り組みは、テクノロジーおよび製品セキュリティに関する以下の 7 つの中核的な柱に焦点を当てています。

1. 多要素認証。
2. デフォルトのパスワード。
3. あらゆる種類の脆弱性を根本的に削減。
4. セキュリティパッチ。
5. 脆弱性開示ポリシー。
6. CVE。
7. 侵害の証拠。

セキュアバイデザインは、透明性を重視するソフォスの理念と一致しており、ソフォスのセキュリティ対策を継続的に評価・改善していくための指針となっています。

ソフォスは、改善に向けたコミットメントを公開し、セキュアバイデザインのフレームワークの 7 つの中核的な柱に対する取り組みの進捗を共有しています。もちろん、サイバーセキュリティは常に進化しており、取り組みが完了することはありません。セキュアバイデザインの原則をソフォスのあらゆる製品に適用し続け、その精度と実効性を高めていくことは、今後も継続的かつ中心的な取り組みであり、ソフォスの理念の中核となています。

ソフォスは、Sophos Firewall のセキュリティポスチャを大幅に強化し、同時にユーザーの負担を大きく軽減する、いくつもの重要なセキュアバイデザインの機能を提供している点で他社とは一線を画しています。Sophos Firewall は、市場で唯一、ダウンタイムを一切発生させずに、セキュリティパッチを OTA (ワイヤレス) で自動適用できるファイアウォールです。さらに、ソフォスは唯一、すべての顧客のファイアウォール導入環境を対象に、攻撃の兆候がないか積極的に監視しているベンダーでもあります。これにより、異常が検知された際には迅速に対応し、ソフォスを利用している組織やサイバーセキュリティパートナーが攻撃を特定・対処できるよう支援するとともに、同様の攻撃から他のすべての顧客を即座に保護することが可能になります。

重要ポイント

セキュアバイデザインは、透明性を重視するソフォスの理念と一致しており、ソフォスのセキュリティ対策を継続的に評価・改善していくための指針となっています。

Sophos Firewall の最新バージョン (v22) では、セキュアバイデザインの機能が拡張され、ファイアウォールのセキュリティポスチャが大幅に強化されています。これらの機能には以下が含まれます。

- 設定ミスにより攻撃を受けるリスクを軽減する新しいセキュリティ状態のチェック機能。
- 刷新されたコントロールプレーン。最大限のセキュリティと拡張性を実現するために再設計されており、特定の種類の脆弱性を根本から排除します。
- Sophos XDR Linux センサーを新たに追加したことで、ソフォスのセキュリティチームがあらゆる顧客環境のシステム整合性をリアルタイムでより高度に監視できるようになり、攻撃の特定と対応をこれまで以上に迅速に行えるようになりました。
- ファームウェアアップデートは暗号化され、真正性を確保するために証明書ピンニングが適用されるようになりました。
- 最新のソフォスマルウェア対策エンジンへアップグレードされ、新たな脅威にも対応するゼロデイ脆弱性のリアルタイム検知が強化されました。

Pacific Rim キャンペーンに対するソフォスの調査によって、高度な資金力と強い意志を持つ攻撃者がどのように活動しているのかを、まさに攻撃の最前列で目の当たりにしました。そして、このような攻撃者に対抗するために本当に必要なものが何であるかを深く理解することができました。このキャンペーンを通じて明らかになったのは、サイバー攻撃者は弱点が露呈するのを待っているわけではなく、設計上の抜け道や設定のギャップ、適用されていないパッチを世界中のインフラから積極的に探し回っているということです。その経験が、ソフォスのセキュアバイデザインのアプローチを直接的に形作る原動力となっています。

これは、現代の防御は製品レベルでアタックサーフェスを削減することから始めるべきだという点を強く示しています。強固なデフォルト設定を組み込み、認証経路を厳格化し、脆弱性が実環境で露呈するよりはるか前に悪用の余地を排除しておく必要があります。

今後に向けて

セキュアバイデザインはすべての脆弱性を排除するものではなく、継続的な警戒が不要になるわけでもありません。しかし、アタックサーフェスを減らすためのサイバーセキュリティにおける基本的な土台です。セキュアバイデザインの有用性は、もはや議論の余地がありません。問われているのは、セキュアバイデザインを取り入れた製品をどれだけ早く採用できるかです。

サイバーセキュリティプログラムの評価を始めましょう

ソフォスの専門家にご相談ください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp

© Copyright 2026.Sophos Ltd.All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK.
Sophos は、Sophos Ltd. の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。